S. Hrg. 109–976

HOMELAND SECURITY: THE NEXT 5 YEARS

HEARING

BEFORE THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

ONE HUNDRED NINTH CONGRESS

SECOND SESSION

SEPTEMBER 12, 2006

Available via http://www.access.gpo.gov/congress/senate

Printed for the use of the
Committee on Homeland Security and Governmental Affairs

U.S. GOVERNMENT PRINTING OFFICE

30–595 PDF WASHINGTON : 2007

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

SUSAN M. COLLINS, Maine, *Chairman*

TED STEVENS, Alaska
GEORGE V. VOINOVICH, Ohio
NORM COLEMAN, Minnesota
TOM COBURN, Oklahoma
LINCOLN D. CHAFEE, Rhode Island
ROBERT F. BENNETT, Utah
PETE V. DOMENICI, New Mexico
JOHN W. WARNER, Virginia

JOSEPH I. LIEBERMAN, Connecticut
CARL LEVIN, Michigan
DANIEL K. AKAKA, Hawaii
THOMAS R. CARPER, Delaware
MARK DAYTON, Minnesota
FRANK LAUTENBERG, New Jersey
MARK PRYOR, Arkansas

ALLISON J. BOYD, *Counsel*
MELVIN D. ALBRITTON, *Counsel*
JENNIFER A. HEMINGWAY, *Professional Staff Member*
MICHAEL L. ALEXANDER, *Minority Staff Director*
HOLLY A. IDELSON, *Minority Counsel*
TRINA DRIESSNACK TYRER, *Chief Clerk*

CONTENTS

WITNESSES

TUESDAY, SEPTEMBER 12, 2006

ALPHABETICAL LIST OF WITNESSES

APPENDIX

HOMELAND SECURITY: THE NEXT 5 YEARS

TUESDAY, SEPTEMBER 12, 2006

U.S. SENATE,
COMMITTEE ON HOMELAND SECURITY
AND GOVERNMENTAL AFFAIRS,
Washington, DC.

The Committee met, pursuant to notice, at 9:32 a.m., in room SD–342, Dirksen Senate Office Building, Hon. Susan M. Collins, Chairman of the Committee, presiding.

Present: Senators Collins, Voinovich, Coleman, Bennett, Domenici, Warner, Lieberman, Levin, Carper, Dayton, Lautenberg, and Pryor.

OPENING STATEMENT OF CHAIRMAN COLLINS

Chairman COLLINS. Good morning. We have a very full agenda today with many distinguished witnesses, so I am going to ask all of us to abbreviate our opening statements because we have a noon vote.

As the Nation remembers the shock and loss of the attacks on our country 5 years ago, the Committee this morning will look ahead to assess the homeland security challenges the next 5 years will bring. Our expert witnesses, from the very top of the Department of Homeland Security to the front lines, will provide valuable insight into these challenges.

The morning of September 11, 2001, was one of uncommon brilliance here in the United States. In the blink of an eye, it was transformed into one of unthinkable horror. Two thousand nine hundred ninety-six innocent men, women, and children perished. Two of our major cities were under assault, two centers of our economic and military power were in flames, as was a field in Pennsylvania. To many, it seemed that a new kind of war had begun.

If we had had the discussion that we are having today 5 years before September 11, 2001, it would have been clear that those attacks were not the opening salvo of a new war, but the foreseeable escalation of a war that had long been underway. Nineteen ninety-six was the year that Ramzi Yousef, while awaiting trial for the 1993 World Trade Center bombing, was convicted of a conspiracy to plant bombs on a number of U.S. airliners. Nineteen ninety-six was the year of the truck bomb attack on Khobar Towers, an attack that specifically targeted U.S. military personnel. And, 1996 was the year that Osama bin Laden relocated from Sudan to Afghanistan and declared war on the United States. The terrorist strategy was evolving to direct massive attacks on high-profile

American targets, but we failed to see it. We failed to perceive that these seemingly isolated events were, in fact, tied together.

That was the failure which the 9/11 Commission referred to as a "failure of imagination." How different things might be today, 5 years after September 11, 2001, if our imagination had been fully engaged 5 years before.

The fundamental obligation of government is to protect its citizens. Today, we will explore a number of questions about how government can better protect its citizens. To answer those questions, we must first seek to identify the threats we face.

Terrorism constantly evolves. As the devastating attacks around the world prove, terrorists will strike wherever opportunity allows and wherever innocent people are the most vulnerable. The terrorists' resourcefulness, cunning, and patience are exceeded only by their cruelty.

The recent arrests in Canada and Miami, the attacks on the London subway last year, and the thwarted airliner plot in Britain have made clear that terrorism masterminds no longer have to rely upon operatives imported from abroad to infiltrate target nations and carry out attacks. The emerging threat appears to be from "homegrown" terrorists, much harder to detect and not deterred by increased security at our borders.

I am particularly concerned by the extent to which this infection is spread within our State and Federal prisons. The Committee will hold a hearing on prison radicalization later this month. But we know from cases both abroad and here in the United States, with Kevin James, an American now awaiting trial who founded an organization based upon his radical interpretation of Islam while in prison in California, that the new face of terrorism may be born and raised right here in America.

As the terrorist tactics evolve, the overall objective remains the same—to cause maximum loss of innocent lives, to damage our economy, and to defeat our resolve. As they adapt to our strengthened defenses, terrorists continue to pursue ever more spectacular and devastating attacks.

In addition to identifying the most likely threats that we face, we must constantly assess and improve our efforts to counter them.

Our efforts during the past 5 years have been substantial. We have closed the gap between law enforcement and intelligence that the terrorists exploited on September 11. We have created the Department of Homeland Security. We have made investments in training and equipping our first responders. We have strengthened our borders with additional personnel and improved technology. We have brought about the most comprehensive restructuring of our intelligence community in more than a half century.

These efforts, though, do not describe a task accomplished but one underway. Each remains a work in progress, and the emerging threats compel us to ask the hard questions about how well we have done in the past and whether we are prepared for the future.

Among the questions that I intend to explore today are:

How can we confront the challenge of homegrown terrorists? What resources do State and local law enforcement need to meet it? How can we work with the American Muslim community to prevent the radicalization of our own citizens?

What are our greatest vulnerabilities to a chemical, biological, or nuclear attack, and how can they be mitigated?

How can we continue to improve the effectiveness of intelligence-gathering capabilities against terrorists while protecting the civil liberties of the American people?

How can we accelerate the development of a common culture at DHS and help DHS work more effectively with its State and local counterparts in detecting, preventing, and responding to acts of terrorism?

What is the role of the private sector—the business community, health, education, and other institutions, as well as the public—in strengthening our defenses against terrorism?

Have we neglected the security of other forms of mass transportation in our focus on aviation security?

How can we use our technological edge more effectively? Should interoperable communications be a national priority? What other technologies can we better deploy to protect against diverse targets?

From the perspective of the past and present, we must imagine the future. September 11, 2001, was a day of profound loss, but it was also a day of inspiring courage. The first responders and ordinary citizens who rushed into the Twin Towers and the Pentagon to save others, the brave souls on Flight 93 who gave their lives so that others might live, remind us of the greatest asset we bring to bear against this challenge—the spirit of the American people.

Chairman COLLINS. Senator Lieberman.

OPENING STATEMENT OF SENATOR LIEBERMAN

Senator LIEBERMAN. Thank you very much, Madam Chairman. Welcome to you, Secretary Chertoff.

Madam Chairman, I am grateful to you for calling this hearing to discuss the state of our homeland security 5 years after Islamic terrorists murdered 3,000 innocent Americans and shocked the rest of us out of our false post-Cold-War sense of security. Yesterday was a day of remembrance and requiem. Today we quite properly ask: Where do we want to be in homeland security 5 years from today? What can we say, if I may personalize it, to the parents of America about what we will do in the next 5 years together to be able to guarantee that their children's upbringing and lives will be as secure as theirs were prior to September 11?

September 11, 2001, like Pearl Harbor, was a tragedy of such enormity that it began a new era in which we understand that we are at war with a different kind of enemy and that our country, led by the Federal Government, must pull together and do better at fulfilling our constitutional responsibility to provide for the common defense against this unconventional and unprecedented threat. The threat of a terrorist attack at home on Americans is as real today as it was 5 years ago. The foiled plot to explode airliners heading to the United States from the United Kingdom is the most recent and publicly acknowledged example.

But let me say at the outset that just as the threat of a terrorist attack is as real today at home as it was 5 years ago, we together can say to the American people that they are safer than they were

on September 11, 2001, although, as we all acknowledge, they are not yet as safe as we want them to be.

We have every reason, as we look back at these 5 years, to thank God and to thank all who work each day to protect our homeland security that America and Americans have not been attacked at home since September 11, 2001. We are thankful that a number of terrorist plots have been disrupted through increased vigilance at home and cooperative work with our allies abroad. And as Chairman Collins has indicated, since September 11, we have made historic organizational changes in our government to shore up our homeland defenses. These include the reorganization of our vast and far-flung security and emergency response agencies into the Department of Homeland Security, the creation of the 9/11 Commission, the enactment of its bold proposals for reform and greater security, and the establishment of the Northern Command to focus the Department of Defense on homeland as well as international security.

The point of these changes has been to focus the Federal Government's attention on terrorism 24 hours a day, 7 days a week with resolve, coordination, and strong leadership to bring purpose and effectiveness to the protection of our homeland. As I have said, we are clearly safer today because of all that we have done together, although there are clearly weak links remaining that we must deal with together.

I know that along the way there have been misgivings and some soul searching about the Department of Homeland Security, but I do not hear any credible voice saying that we erred in creating the Department of Homeland Security. So if the Department has not yet fully lived up to all that we in Congress hoped it would be, let us resolve today, as we look forward to the next 5 years, to work together to make it so.

Let me say very briefly that the first great challenge that the Department has faced is to bring itself together. We gave the Department an enormous task to bring together 180,000 Federal employees from a large number of agencies with different cultures and different directions. I quote Warren Bennis here, adviser to four Presidents, who said that we need "the capacity to translate vision into reality." And that is the work of leadership, and it has been a challenge, but I believe progress has been made in the time that the Department has existed.

The failure of leadership we saw, without belaboring, acutely and tragically in the run-up and aftermath to Hurricane Katrina. Mr. Secretary, as you know, the pain and devastation that Hurricane Katrina caused and is still causing would be even worse if a weapon of mass destruction, a nuclear weapon, were to explode in a crowded city, if terrorists were to spray a mall with a deadly biological agent, or if a naturally occurring virus spread to the level of a pandemic. We are looking to you for leadership on these threats. I know that you have acted to apply some of the painful lessons learned in Hurricane Katrina. You know that we on this Committee have tried to do the same through legislative work. The fact is that there is more work to be done.

Second, I continue to believe that we are underfunding some of the critical homeland security needs, particularly our first responders.

Mr. Secretary, today I look forward to hearing from you, to use Bennis' words, your vision of where this Department is going, but also what you intend to do to translate that vision into reality and into action. I also welcome and look forward to the views of the expert witnesses who will follow.

The security of the American people is the highest priority of our government. The plain fact is, without security, there cannot and will not be the life, liberty, and pursuit of happiness that our government was formed to secure. So we have got to get this right, and we have got to get it right together.

And I close with a thank you to Chairman Collins and the other Members of the Committee because, as we look back over the last 5 years since September 11, 2001, in a capital city, which has become all too partisan, reflexively, on the question of homeland security—and there have been moments where this has not been totally true, but on balance, as we look back, this Committee has acted with a real sense of unity that goes well beyond partisanship for the national interest and for homeland security. And the legislation that we have reported out, that has been adopted by Congress, that has been signed by the President, and that I believe today makes the American people safer than they would otherwise be is a testament, Madam Chairman, to your leadership and to the commitment of all Members of the Committee to forget party labels and work together as Americans to secure our future against a brutal and inhumane enemy.

I thank the Chairman.

Senator COLLINS. Thank you, Senator.

Senator Domenici has asked to give his statement next because he has to leave for another committee that he is chairing.

Senator Domenici.

OPENING STATEMENT OF SENATOR DOMENICI

Senator DOMENICI. Let me thank you so much and say to the other Members, I will take little time. I have to chair the Energy and Natural Resources Committee hearing wherein we have the company involved with the Alaskan spill. That is the issue before that committee, and I am chairing it, so I would ask that my statement be made a part of the record, Madam Chairman.

Chairman COLLINS. Without objection, all statements will be.

Senator DOMENICI. I would just say to the Secretary, I commend you for the work you are doing, and my observation as one who works here on the Committee and observes from the outside is that things are beginning to gel in the way you would like to see them. It is a very difficult job that you have taken on, and I know it is not always successful day by day. But I want you to know that I always thought you had the potential to be a great leader in this job. And I want to continue to give you the opportunity to prove what you can do.

I also look forward to seeing you more and more on the science and research part of your endeavor because that is absolutely paramount. Some things are happening with our National Laboratories

that seem to me to bode well for our future and send some terribly tough signals to our opposition that we are up to finding out what they are doing and we are doing something about it. For this I thank you and congratulate you.

I think I will see you in my State at a dedication of an R&D facility, which does make me think very highly about your capabilities in the future. Thank you.

Thank you to all of the Senators.

[The prepared statement of Senator Domenici follows:]

PREPARED STATEMENT OF SENATOR DOMENICI

Madam Chairman, thank you for holding this hearing to discuss the Department of Homeland Security's future. Thank you also, Secretary Chertoff, for spending time with us today to discuss the future of homeland security.

I want to start by thanking you for taking on the difficult task of overseeing the Department of Homeland Security. Your Department is young and is tasked with the difficult job of securing our Nation. I appreciate your service to America, I have enjoyed working with you over the past couple of years, and I look forward to working with you in the future.

It is appropriate that we meet today to discuss homeland security since yesterday was the fifth anniversary of September 11, 2001. That was a horrific day, and the images and shock are still with us. But I believe that since then, we have made significant progress in the Global War on Terror and in our efforts to secure America.

I look forward to hearing about where we have come since establishing the Department of Homeland Security in 2002 and where we are going in the coming years. I believe our future will include new research and development efforts; collaboration with universities, industry and national labs; secure borders and ports of entry; and state-of-the-art security technologies. This isn't an exhaustive list of our homeland security needs, and I look forward to hearing from our witnesses on the future of homeland security.

Thank you, Madam Chairman.

Senator COLLINS. Senator Levin.

OPENING STATEMENT OF SENATOR LEVIN

Senator LEVIN. Thank you, Madam Chairman, and thank you for calling this hearing and for the way that you and Senator Lieberman have managed to run this Committee on such a wonderfully bipartisan and effective basis.

Immediately following the September 11 attacks, America came together as one Nation with one purpose: Protecting our country from those who would do us harm. Since that time, we have made important progress, such as hardening airplane cockpits and federalizing aviation security. Yet 5 years later, there are still gaps in our homeland security system that need to be closed. The focus of this hearing is to look forward and to ask what still needs to be done.

First, if we are serious about homeland security, we need to adequately fund it. Year after year, we have seen significant cuts to our vital first responder grant programs. One of the areas where we have a significant shortfall is in the area of interoperable communications equipment. In the Senate, we have voted to establish demonstration projects for interoperable communications along Northern and Southern borders, but those projects have been dropped in conference. We still do not have a dedicated source of funding for interoperable communications equipment within the Department of Homeland Security, and presumably that means

that the Administration does not believe that interoperable communications are important enough to deserve dedicated funding.

Another major shortfall is in the area of reducing the threat of proliferation of fissile materials. The 9/11 Commission found that the "greatest danger of another catastrophic attack in the United States will materialize if the world's most dangerous terrorists acquire the world's most dangerous weapons." The report went on to state that al-Qaeda has tried to acquire or make weapons of mass destruction for at least 10 years and that there is no doubt that the United States would be a prime target. Preventing the proliferation of these weapons warrants a maximum effort by strengthening counterproliferation efforts, expanding the Proliferation Security Initiative, and supporting the Cooperative Threat Reduction Program.

In the December 2005 follow-up report card, the 9/11 Commission gave the Administration a grade of D on this recommendation, saying that, "Countering the greatest threat to America's security is still not the top national security priority of the President and the Congress."

We also have great needs, I believe, particular needs in the area of developing a consolidated watchlist of persons that are suspected of terrorism, where terrorists are identified and stopped from entering into the country and moving around our country. Five years after the September 11 attack, we still have a long way to go, according to the Government Accountability Office, in compiling a watchlist that is complete, accurate, and available to law enforcement.

I want to thank Secretary Chertoff for joining us today and, again, thank you, Madam Chairman, and our Ranking Member, Senator Lieberman. And I hope we can continue to all work together to accomplish these important objectives.

Chairman COLLINS. Thank you. Senator Coleman.

OPENING STATEMENT OF SENATOR COLEMAN

Senator COLEMAN. Thank you, Madam Chairman. I agree with your comment and that of the Ranking Member that we are safer today, but we do live in a much more dangerous world. I just want to thank you for this hearing, looking forward 5 years. All too often in the Senate, we have focused on yesterday, today, and if we are lucky, maybe tomorrow. This is important enough to look down to the future.

A principal responsibility of government, Madam Chairman, as you noted, is protecting the citizens and providing for the national security. And in this post-September 11 world, Mr. Secretary, that is homeland security, your responsibility, which is right at the very center. In the past, we suffered from a failure of imagination. Today we have to worry about the failure to deal with the unimaginable. We have to imagine the unimaginable and then figure out a way to deal with it, and that is an extraordinary challenge, and the challenges are broad—border security, port security, chemical security, just to name a few.

We also must rebuild the confidence of the Department of Homeland Security and its ability to respond to disasters both natural and manmade. We cannot ignore that and must ensure that bu-

reaucracy and red tape don't hinder the ability to integrate new technologies. There is great hope with new technologies. Senator Domenici talked about that. It is also a key to success.

Finally, we need to remember the lessons of September 11, 2001, and the decade that preceded it. As the Chairman has noted, we cannot rest, we cannot let our guard down, and we cannot relent in fighting this battle that history will reveal as the battle of our lifetime. And I am confident that with strong leadership and a bipartisan effort we will succeed.

Thank you, Madam Chairman, and I would ask that my full statement be entered into the record.

Chairman COLLINS. Without objection.

[The prepared statement of Senator Coleman follows:]

PREPARED STATEMENT OF SENATOR COLEMAN

I want to thank our distinguished Chairman and Ranking Member for holding this important hearing.

We have the opportunity today to make an assessment of where we are, and equally important, where we are going in terms of homeland security over the next 5 years. The facts are that today America is safer than it was on September 11, 2001. It is a major accomplishment that there have not been any successful terrorist attacks on American soil in 5 years and this is a testament to the great lengths we have gone to protect our citizens both at home and abroad. It is also a testament to the strength, vigilance and awareness of the American people.

Additionally, the creation of the Department of Homeland Security and the revamping of our intelligence community operations have institutionalized and improved the practice of defending our Nation. As a result, 15 major terrorist plots against America have been thwarted—and those are just the ones that have been disclosed. Countless more undisclosed plots are likely to have been thwarted as well. However, we face an enemy that is constantly adapting and changing and that only has to be right once where we have to get it right 100 percent of the time.

With this in mind, a strategic vision for the future must have some built-in flexibility so that we have the ability to change as our enemies do. There are certainly many challenges that lie ahead including border security, port security and chemical security, just to name a few. We must also rebuild the confidence of the American people in the Department of Homeland Security's ability to respond to disasters both natural and man-made. Ensuring that bureaucracy and red tape do not hinder the Department's ability to integrate new technologies and ideas to address these issues will be a key to future success. Finally, we need to remember the lessons of September 11 and the decade that preceded it. We cannot rest. We cannot let our guard down. And we cannot relent in fighting this battle that history will reveal as the battle of our lifetime.

I look forward to hearing the testimony from our witnesses today and again want to thank the Chairman and Ranking Member for their leadership on this issue.

Senator COLLINS. Senator Dayton.

OPENING STATEMENT OF SENATOR DAYTON

Senator DAYTON. Thank you, Madam Chairman.

Mr. Secretary, when Minnesotans ask me, as they often do, whether we are safer since September 11, I reply that we are because of the constant vigilance of yourself and thousands of other dedicated men and women in your agency and our Armed Services, our intelligence agencies, and so many others. And I salute you and all of them for your dedicated efforts.

That being said, we must continually ask ourselves what can we do better, and in August, just last month, I toured parts of our Southern border with Mexico in Texas, New Mexico, Arizona, and our Northern border with Canada along northern Minnesota. On our Southern border, I met with many experienced and sophisti-

cated Federal agencies who, frankly, should be heard by this Committee and by Congress regarding what is effective and what is not for our border security. However, my eyewitness experience supports Senator Lieberman's statement that we are underfunding our border security efforts.

For example, in El Paso, Texas, the day before my early morning visit that one facility apprehended and detained 269 people attempting to illegally enter our country. There is a fence, which is one of the important barriers to that illegal entry, yet still within the city limits that fence inexplicably just stops. The reason, I was told, is because the funding had run out.

Along our Northern border, the Federal homeland security presence is far more limited, and in long stretches of that 5,525-mile border, border security is really non-existent. Despite increased funding by Congress and a mandate to increase the number of Northern border agents during the past 2 years, that number of border control agents has reportedly declined from 996 to 950. At any one time, only 250 agents are actively guarding our Northern border, and local law enforcement officials, whose first responder funding in Minnesota has been cut to only 40 percent of what it was a year ago, tell me that the Federal presence, while the people individually are very dedicated, is simply not sufficient to meet the demands. The illegal trafficking of people, of narcotics, of, God forbid, terrorists, while not as strong a likelihood as along our Southern border, and certainly the volume of what they call "economic illegal immigration," those coming across the country for job purposes, is far less, still the threat is very real. And I would commend to you, as others have said, the need to increase that Northern border security.

I would ask respectfully that you and the President—and I have written the President, asking for your support of an amendment which I had introduced, which was adopted by the Senate, which would increase the funding by $44 million for Northern border security agents, increase the number by 236, which would be a 24-percent increase. That is in the fiscal year 2007 Senate appropriations bill that is going to conference. I would again respectfully ask for your support and that of the Administration. That would be an important first step to improving our Northern border security.

Thank you, Madam Chairman.

Chairman COLLINS. Thank you. Senator Warner.

OPENING STATEMENT OF SENATOR WARNER

Senator WARNER. Thank you very much, Madam Chairman. I will put my statement into the record, but I do want to join in a most sincere way in commending you and Senator Lieberman for the strong leadership that you have given this Committee on a most critical issue. I do not know of anything more critical than our own homeland security. Both of you are members of the Armed Services Committee, so you bring that perspective to bear on this.

I also want to commend the President for the manner in which he led the Nation yesterday in, I think, very respectful ceremonies honoring those who lost their lives and reminding America about the enemy we face today is unlike any enemy that we have ever faced in the history of this Nation in terms of the breadth and the

depth and the blind conviction that they have to bring destruction to those people in the free nations of the world, and most particularly, I suppose, us.

But I would say also, Secretary Chertoff, you have shown strong leadership. You have weathered the storms, and your strength of leadership seems to grow daily. And I commend you for the manner in which you found time during the summer period to travel extensively across this Nation, indeed to my State. And I watched you firsthand dealing with those first responders, be they policemen or firemen or other people in the communities, and struggle with the tough questions put down at the grass-roots level. You had the answers. You gave the assurances. But you were realistic and honest in your approach about how funds are not unlimited, but you are doing the best you can to distribute them. So carry on.

But I would come back to a caution by my good friend, Senator Levin. Both of us are concerned about the progress made in establishing more robust interoperability of communications, and I would hope in your remarks today you would address that.

I thank the Chairman.

[The prepared statement of Senator Warner follows:]

PREPARED STATEMENT OF SENATOR WARNER

Madam Chairman, thank you for calling this hearing today and I wish to thank our witnesses for their efforts over the past 5 years to help make our Nation a more secure place. Much has been done to date at the local, State, and Federal levels. The formation of the Department of Homeland Security combined dozens of Federal agencies; created new agencies and directorates; and established a comprehensive Federal mission for the new paradigm of security risks our Nation now faces. The 185,000 public servants of DHS are dedicated to their mission to protect this country, its people, and its ideals from those who mean to do harm.

We have taken significant steps in critical infrastructure protection; enhanced transportation security on land, sea, and air; strengthened security at the Nation's borders and ports; reformed our intelligence capabilities; and established a stronger coordination of effort among the various levels of government.

But perhaps the single most important change in this country over the past 5 years is one that each individual American has experienced in his or her heart and mind. It is simply the realization that we are not safe from those who mean to do us harm and that we can never again rest from the charge to protect our home. Today's enemy is different than those of the past. No longer are we dealing with actual governments as the primary threat—we must now defend our own cities from within.

I joined this Committee in the 109th Congress because I fervently believe that this is a critical time in American history not unlike when the branches of the military were combined into one Department of Defense in the 1940's. We continue to build the Department of Homeland Security to lead efforts to protect the Nation and under the leadership of former Secretary Ridge and now Secretary Chertoff we are in good hands.

Five years ago I said that "our people have suffered in a single day our greatest tragedy—yet history will show this to be America's finest hour." I look forward to hearing from our witnesses today and continuing the work before this Committee to enhance the safety and security of our entire Nation.

Senator COLLINS. Senator Voinovich.

OPENING STATEMENT OF SENATOR VOINOVICH

Senator VOINOVICH. Thank you, Madam Chairman.

First of all, I would like to say this: The question I am constantly asked when I am at home in Ohio is, "With such partisanship in Washington, how can Congress accomplish anything?" And I point to this Committee and several other committees where bipartisan-

ship is well and alive. And I commend you and Senator Lieberman for the terrific leadership that you have provided to this Committee. The American people should be assured that we are working together on the very important homeland security challenges that face our Nation.

Second, yesterday, I think standing on the steps of the Capitol in memory of September 11, 2001, vividly reminded me of the serious threats we are facing in the global war on terror, and I think most people thank God that we have not had any terrorist event here in this country for the last 5 years.

I am pleased also that the President has finally leveled with the American people and indicated that we are at war. Osama bin Laden has declared war on us. Our freedom and way of life is under attack by Islamic extremists who have distorted the Islamic faith and launched jihad against the United States and anyone who shares our values. And the American people should understand that this is the situation. I sometimes refer to it as the "Fourth World War." In other words, this struggle is not something that is going to be over by snapping our fingers. It is going to be with us now for a long time. I would hope that maybe my grandchildren will have this off their back, but it is going to take a lot of hard work.

Our success in the war on terror has much to do with the Homeland Security Department, which has been in existence now for over 3 years. I think people should understand that it is the most formidable management challenge ever undertaken in the United States of America: Merging 180,000 people and 22 disparate departments and programs, and it is not going to be a lay-up shot to integrate this new Department. And it is not going to be fully accomplished, Secretary Chertoff, during your term. The management challenges will continue for quite some time, and it will take significant effort and focus to ensure that the Department becomes all that we want it to be.

We must also understand that we cannot guard against every security threat imaginable. We need to recognize that we have astronomical national debt, and it is the highest percentage of our GDP in a long time. We are neglecting the nondefense discretionary part of our Federal budget. We have to look at the big picture and prioritize based on our limited fiscal resources. I don't know how we can continue overspending in this country.

From a fiscal point of view, we simply cannot afford to accomplish every objective Congress is seeking to achieve. We need more budgetary resources, perhaps even a temporary increase in our taxes so that we can afford to address our enormous national debt, improve our homeland security capabilities, and also continue fighting the wars in Afghanistan and Iraq. Secretary Chertoff, constantly Congress is telling you, do this, do that. You only have so much money, and we need to consider the big picture, the whole budgetary perspective, and better prioritize our homeland security spending according to risk.

Secretary Chertoff, today I am also hoping that we can hear from you about your strategic plan for the Department. Where are you now? Where are you going? How long is it going to take? And how can we help you to better do the job that we have asked you to do?

[The prepared statement of Senator Voinovich follows:]

PREPARED STATEMENT OF SENATOR VOINOVICH

Yesterday, our Nation observed the fifth anniversary of the tragic and violent terrorist attacks of September 11, 2001. The brutal images of September 11 will forever be burned into the minds of the American people. My own memories of visiting the Pentagon and being at Ground Zero shortly after the attacks will never fade.

Each anniversary of September 11 renews our national resolve to fight the War on Terrorism at home and abroad. The American public should be reassured that our Nation is undoubtedly safer, but we must remain vigilant, because Osama bin Laden has declared war on us. Our freedom and way of life is under attack by Islamic extremists who have hijacked the Islamic faith and launched a jihad against the United States, Israel, and anyone who shares our values.

Madam Chairman, thank you for holding this important hearing today to evaluate the Federal Government's progress in securing the American homeland against future attacks. Five years after September 11, and more than 3 years after the creation of the Department of Homeland Security, it is appropriate for this Committee to take stock of our national homeland security policy and evaluate where we are and where we need to be.

Integral to this discussion is a review of how the Department of Homeland Security is coming together as a cohesive entity. As my colleagues know, the creation of DHS in 2003 merged 180,000 employees from 22 disparate Federal agencies and represented the single largest restructuring of the Federal Government since the creation of the Department of Defense in 1947.

Building stronger management capabilities is vital to the success of the Department. In order to effectively accomplish its complex mission of securing the Nation from terrorism and natural hazards, DHS must have an effective management structure with experienced leaders who are capable of integrating the many separate departmental components and ensuring effective operations and planning.

I hope today's hearing will also include a thoughtful examination of ways we can improve our risk management capabilities. We all agree that it is imperative to secure our homeland against terrorism and strengthen our response capabilities, but we must also acknowledge that this country has finite budgetary resources.

It is simply not possible for us to guard against every theat—and frankly, if we tried to, we would bankrupt our Nation in the process. As our national homeland security policy matures, we have to use our common sense and begin to prioritize by allocating our limited resources based upon risk assessments.

Secretary Chertoff, thank you for being here and for your service to our Nation. I look forward to your testimony regarding the progress DHS has made and what I hope will be a candid discussion of the challenges the Department continues to face. Thank you, Madam Chairman.

Chairman COLLINS. Thank you. Senator Bennett.

OPENING STATEMENT OF SENATOR BENNETT

Senator BENNETT. Thank you, Madam Chairman.

The war with terrorists did not begin on September 11, 2001. It was going well before that, just as the Second World War did not begin on December 7, 1941. Those were the two dates on which Americans became aware of the fact that war was going on in the world around them and the two dates on which it came home to Americans in a very terrible and terrifying kind of way.

During and after the Second World War, we reorganized our resources and our government to deal with the threat that we discovered, and we are doing the same thing now, reorganizing our government to deal with the threat that we have discovered. It was not easy after December 7, 1941, and it has not been easy after September 11, 2001, but it is a task that we must be about. And, Madam Chairman, you and Senator Lieberman have led the way in this Committee.

Secretary Chertoff, you have the burden of presiding over one of the most difficult parts of this reorganization around the new reali-

ties in the world. You are handling it in a very capable fashion, and we appreciate your service. We appreciate your dedication to this task and look forward to hearing what you have to say.

Chairman COLLINS. Thank you. Senator Carper.

OPENING STATEMENT OF SENATOR CARPER

Senator CARPER. Thanks, Madam Chairman. Mr. Secretary, good morning.

I want to start off by thanking Madam Chairman and our Ranking Member for holding this hearing this morning. It is certainly a timely one.

Five years ago yesterday, as we all know, the prevention of future terrorist attacks like the one that occurred for all intents and purposes became the Federal Government's, our government's top priority. And it became a top priority for State and local governments like my own State of Delaware. And as we reflected yesterday on the tragedy that struck us 5 years ago, I think it is good that we are also taking the time here today to examine the progress that we have made and, in some cases, the lack of progress that we have made since that tragic day occurred.

There has been progress in a number of areas. As I travel in airplanes, I am reminded, especially coming back from Manchester, England, a couple of weeks ago, of our ability to respond quickly and to try to tamp down threats that would harm many people at once.

As I visit nuclear power plants—and I have visited several around the country—I am reminded I think we are doing a better job there in making them more secure.

As we look at our ports, I think we have done some good. I think we can do more in the legislation that we take up today, that our Chairman and Ranking Member and Senator Murray have worked a whole lot on, but there is a good deal more that we can do there. There is a good deal more that we can do with respect to rail and transit security, and we have an opportunity to consider that in the context of the port security bill.

This Committee has worked long and hard on trying to make chemical plants more secure, and I do not know that we will have a chance to take that bill up this week, but we need to get the bill reported out of Committee almost unanimously and get it before the full Senate.

I look forward to hearing from you, Mr. Chertoff—I always do, Mr. Secretary—and from our other witnesses today about the successes of the last 5 years but, more importantly, about the work that you and your Department need to do and what we need to do to support those efforts, and hopefully to improve them.

For a variety of reasons, whether it be the war in Iraq or the continuing standoff between Israel and the Palestinians or any number of other grievances, the number of those who wish to do us harm is likely growing, and it is important that we get this right.

Thank you.

Chairman COLLINS. Thank you.

We are now very pleased to welcome our first witness today, the Secretary of the Department of Homeland Security, Michael Chertoff.

TESTIMONY OF HON. MICHAEL CHERTOFF,[1] SECRETARY, U.S. DEPARTMENT OF HOMELAND SECURITY

Secretary CHERTOFF. Chairman Collins, Ranking Member Lieberman, Members of the Committee, it is a real pleasure for me to appear before you today, the day after the fifth anniversary of September 11, 2001, to talk about where we have come over the last 5 years and, perhaps even more important, what our vision is and our strategy is for the next 5 years.

Every time we have a ceremony recalling the events of September 11, 2001, I am reminded of some new way in which it touched each of us, not only in our professional capacities, but in our personal capacities.

Yesterday, as part of my commemoration of September 11, I was in Bayonne, New Jersey, and present at the unveiling of the sculpture given by the Russian people to commemorate the event. I was with Senator Lautenberg from the Committee and former President Clinton and a number of other people. And as we laid the flowers down at the base of the monument at the conclusion of the ceremony, I found the name of a college classmate whose name I had never seen on the rolls of the lost of September 11. And it was a reminder of the fact that the pain of September 11 continues to touch us even 5 years after the event.

But it is also an opportunity to renew our dedication and our unity of purpose. I agree with what everybody here has said. The area of homeland security is one that stands above the normal division of differences that sometimes characterizes what goes on in our political system. It has always been a pleasure for me to work with this Committee because, not only as a group but individually, you have each afforded me wise, dispassionate counsel and always recall that whatever our disagreements, there is a far more central unity of vision that we all have about what we need to do. And so I am delighted to be able to appear at this very momentous time to recall where we have been and see where we are going.

I would say there is one dynamic that is the most important in setting our strategy and our agenda going forward, and that is a recognition that we have to be realistic about what we expect and about what we do. We do have limits, and we do have choices to make, and it falls to me in my job most often to have to make a judgment about how to allocate priorities among those choices.

Our limit is not only financial, although that is clearly a limit, and to understand that, one need look no further than bin Laden himself, who said soon after September 11 he wanted to bankrupt us. He understood that one tool he had in waging war against the United States was to drive us crazy into bankruptcy trying to defend ourselves against every conceivable threat.

But, in addition, we have to bound ourselves with other limits. We do not want to break the very systems we are trying to protect. We do not want to destroy our way of life trying to save it. We do not want to undercut our economy trying to protect our economy. And we do not want to destroy our civil liberties and our freedoms in order to make ourselves safer. So it falls to us in all of these

[1] The prepared statement of Secretary Chertoff appears in the Appendix on page 59.

respects to seek balance and realism about what we can expect, what we promised the American people.

Let me say that I have divided the task into five general buckets, and I will tell you very briefly—and I would ask that my full statement be made part of the record.

Chairman COLLINS. Without objection.

Secretary CHERTOFF [continuing]. Where we have gone and where we intend to go on each of these five buckets.

The first of these is keeping bad people out of the country. This was a central recommendation of the 9/11 Commission. The good news is we do have integrated terrorist watchlists which do enable us to identify the names of bad people who are trying to get into the country. We have also fully deployed our biometric US–VISIT Program, which captures two fingerprints from every non-American who enters the United States and allows us to check them against our databases. That has kept out a lot of bad people.

Between our ports of entry, we have committed to doubling the number of Border Patrol by the end of 2008. We have committed to building additional fencing and additional tactical infrastructure. And we are within 2 weeks about to unroll a strategic technological initiative with respect to the border that will put sensors and unmanned aerial vehicles and other high-tech tools in place to leverage our capabilities and the hard work of our Border Patrol.

We have more we can do. The great challenge, I think, for the next 5 years is not keeping out the known terrorist. It is keeping out the unknown terrorist, the unidentified terrorist. And we have two programs underway that will let us do that.

The first is we need to be able to take passenger name record information, which is information that the airlines capture or travel agents capture, and we need to be able to run that against our databases, against telephone numbers and credit cards that we have already identified as connected to terrorist activity. As we sit here, we have the capability to do that. There is one restriction. The Europeans, up until recently, had restrained our ability to use the information we got from airlines flying from Europe to the United States by limiting the way we could apply that against our databases. We are now in a position where I think we will have an opportunity to talk to the Europeans about modifying those restrictions. Clearly, we need to respect the interest and privacy, but I can tell you from my personal experience after September 11, we used some of that very data to track down the connections of the 19 hijackers in the days immediately following September 11. I was involved in doing that personally. And one of the lessons I learned was this: I would much rather track down the terrorists before the bombs hit than after the bombs hit. And we need to move forward with this.

Second, we are going to start deploying this fall the capability to read 10 prints and not just two prints from foreigners entering the United States. The ability to go to a 10-print system will give us a capability we have not had up to now, which is we can screen all of those prints against latent fingerprints picked up in the battlefields all over the world, in safe houses and off of bomb fragments. It will mean that once this is fully deployed, hopefully with the next couple of years, anybody who has ever been in a safe

house or built a bomb is going to have to wonder whether we are going to catch them when they cross our border.

The second area is screening cargo. Here again I am pleased to say that by the end of this year, we will have 80 percent of the containers that come into the United States going through radiation portal monitors, and by next year we are going to be at close to 100 percent.

Our next vision is to take this overseas, and I know Senator Coleman had suggested I go to Hong Kong. I have looked at the process they have in place there, which is an integrated system for not only screening for radiation but putting containers through X-rays. And we are currently working very actively with a number of foreign ports to begin deploying a system like that over the next couple of years as well.

The third area is infrastructure protection. I am pleased to say we have done a tremendous amount to improve aviation security, as underscored most recently by the events of last August. That includes, contrary to some misinformation that has been put out in the media, that we do have a unified watchlist, the no-fly list that captures all the people whose identities we know about that we want to keep off airplanes. But we also have more work to do with respect to other sectors of transit.

I am pleased to say that next month, in October, I anticipate that the Department of Transportation and my Department will roll out additional and new regulatory measures that will strengthen our ability to control and protect hazardous inhalation materials that travel by rail. I can also say that we have done quite a bit to strengthen our screening of air cargo. One hundred percent of the packages that are presented to the airlines by individuals to be put in the cargo holds of passenger planes are now going to be screened through baggage explosive detecting equipment. And we are working with freight consolidators to increase the amount of screening we do of their freight as well as to insist that they have a trusted traveler program.

The fourth bucket is information sharing. Under the leadership of the DNI, we have done a tremendous amount to improve the collection and sharing of intelligence. I agree with the observations made here, and I think to be made by the next panel, that we need now to work more closely with State and locals in opening up a broad channel of exchange of information. Ambassador McNamara, who is working for Ambassador Negroponte, has been working closely with my chief intelligence officer and the FBI to put such a model in place, and we are already beginning, by embedding our analysts into the field, working with local authorities in fusion centers from Los Angeles to New York, and that program I think has a great deal of hope and a great deal of promise in terms of our ability to build a degree of integration vertically that will match what we now have horizontally.

Finally, let me talk a little bit about response, in particular, the question of interoperability. That, of course, was a central lesson of September 11. The good news is we actually now have technology that will permit first responders and people from different jurisdictions to talk with one another even though they operate radios on different frequencies. These devices are called "gateways," and I

have seen them operate, and they do, in fact, work. That is not to say that we do not want to progress to the next level of technology, which will be a broader ability to use interoperability with different kinds of data that will require us to make some tough decisions about how we use the next stage of digital communications equipment. But it also means that the real challenge now is a challenge of leadership. These agencies have to agree on common rules of the road about how they are going to talk to one another, what codes they are going to use to describe events, who is going to talk to whom, what is the language that is going to be used, and what are the rules of the road.

This is not, frankly, a technology issue. This is an issue of having community leaders come to an agreement. Some communities have done it. We have a lot of interoperability in the National Capital Region. Los Angeles County has interoperability, and they have reached these agreements. Some communities have not done that yet, and we have to guide them in doing that, and we plan to be doing that this year.

Let me conclude by identifying three areas where I think Congress can act this fall to dramatically enhance our ability to continue to build on the progress we have made.

The first is in the area of chemical security. This Committee has done a lot of work on chemical security. It is an urgent issue. One of the great remaining threat vectors for this country is the possibility of somebody attacking our chemical infrastructure and creating an inhalation hazard. We partly regulate this now through our ability to regulate the ports and through the regulation that we are going to be putting out with respect to rail transit in the next month. But there remains a gap, and legislation that is currently in Congress that would address that gap is urgently needed. And I would really request that Congress act on it this month.

Second is port security. I recognize there is legislation on the floor now. It would institutionalize and strengthen many of the measures we are currently taking. We have worked with this Committee on port security. We commend it for its work again. This would be a tremendous contribution to put into effect this month.

And, finally, with respect to the area of immigration, we continue to believe it is important to have a comprehensive plan to address the issue of immigration if we are really going to solve the problem at the border.

There are also some short-term things that can be done. We have recognized the Senate has enacted $1.8 billion in additional funding as part of the Department of Defense supplemental, which would be addressed to strengthening some of what we do in border enforcement. I have also urged again and again that Congress act to dissolve the Orantes injunction, which is hampering our ability to remove people from El Salvador based upon a court order that arises from a civil war that has long ended. Steps like these taking this forward would be of major assistance to us in accomplishing the ambitious but, nevertheless, achievable goals that we have set for ourselves.

Chairman COLLINS. Thank you, Mr. Secretary, for an excellent statement.

You emphasized in your statement the actions that you have taken or will be taking to strengthen border security, which is certainly a goal that I share. But since September 11, the majority of terrorist attacks overseas have been executed by homegrown terrorists. In fact, as Richard Falkenrath will point out on our next panel, "Since September 11, 2001, most terrorists plots and attacks perpetrated worldwide have been conceived, planned, and executed by individuals who are part of the local population and who have had only limited, if any, transnational linkages to terrorist organizations abroad."

The NYPD as well as the L.A. Sheriff's Department have gone to great lengths to establish and deploy counterterrorism units in order to protect their regions against the threat of homegrown terrorism. How much emphasis is the Department placing on this emerging threat?

Secretary CHERTOFF. Chairman Collins, we are putting a lot of emphasis on that threat. We recognize, of course, that the high-consequence threat—the weapon of mass destruction—is still largely a threat that is international in character. But, nevertheless, as demonstrated by what happened in London in 2005, the homegrown threat is serious. We are doing several things.

First of all, we are working with communities like New York and Los Angeles to help them build fusion centers. We opened one in Los Angeles a few months ago, and that is a way of integrating local intelligence gathering with our Federal effort so that we can have a two-way flow of information.

The second thing we are doing is we are particularly focused on prisons. I have met with corrections authorities in New York State and California, where we have, obviously, significant prison populations, to make sure that our intelligence folks are working with their corrections folks at a State level as well as a Federal level to identify threats within the prison system, which history tells us is a fertile breeding ground for extreme groups. And, obviously, prisons are also populated by people who tend to have a willingness to commit acts of violence.

The third thing is we are working hard to understand how it is that homegrown groups get radicalized and become operational. This country has a natural advantage in the way its society operates that has apparently made us much less susceptible than some countries in Western Europe. But it requires that we continue to pay attention to what causes radicalization, that we continue to embrace our Muslim co-citizens, we continue to emphasize the importance of not allowing ethnic prejudice to creep into what we do, so that we tamp down on any tendencies in our own society that might, in fact, replicate what we have sadly seen overseas.

Chairman COLLINS. If you talk to State and local law enforcement officials, over and over again they point to the need for interoperable communications equipment. You have mentioned today that they, too, need to step up to the plate and establish common standards, but there is another obstacle, and that is funding. It is very expensive to establish interoperable communications, and yet many of us think that doing so should be a national priority.

Some of us have suggested designating 25 percent of the homeland security grant money for interoperable communications equip-

ment. Would the Department support dedicated funding to achieve a nationwide goal of interoperable communications so that our first responders will no longer be hampered in their ability to communicate during a disaster? This was one of the lessons from the attacks on our country 5 years ago, but it is a lesson that we saw once again in the response to Hurricane Katrina when within the various parishes in New Orleans the equipment was not compatible.

Secretary CHERTOFF. Well, we have put hundreds of millions of dollars into grant programs for this kind of equipment, and in principle, I think, making sure that our homeland security funds are significantly dedicated to this kind of equipment is worthwhile.

But I do have to say this: Often when I push on this issue, what I see is the problem is we cannot get agreement about what equipment to buy. And perhaps the answer is we will at some point have to simply mandate that this is the equipment you must buy and you are not going to get money for anything else.

But I would hesitate to dedicate a huge amount of money up front without the input of the localities themselves to make a determination of what they feel they need and how far they have come and what the remaining gaps are.

I will say that we are planning by the end of this year to have done a careful study with each of the communities of exactly what their shortfalls are with interoperability. And once we have that done, we may be able to give you a much more specific answer about what funding needs are required.

Chairman COLLINS. But hasn't the Department been working on common standards? It is my understanding that the Federal Government has been working to develop consensus-based equipment standards for 15 years, and now that responsibility is hosted in DHS. So isn't an answer to that problem for the Department to conclude its work and issue the consensus-based standards?

Secretary CHERTOFF. It is, and one thing we are going to do is, as we look at the new digital equipment, we are—and I have actually mandated that we do come up with a standard about the specifications on the digital equipment. One thing I want to make sure of when we do it is that we do not unintentionally lock in a particular proprietary form of communication that gives somebody a monopoly. So we may require that a condition of being designated is that you become open source and you make the proprietary technology available to others so we can have a competitive system.

So I do agree that is something we need to get done. That is to get to the next level. What I do want to emphasize, though, is as we speak at this moment, there is bridging technology that achieves interoperability, and that is available. And if something were to happen tomorrow, that is out there. What needs to be done is those communities that have not finished making their arrangements have to reach an agreement.

Chairman COLLINS. Thank you. Senator Lieberman.

Senator LIEBERMAN. Thanks, Madam Chairman. Thanks again, Secretary.

You spoke at the outset of your statement, I think understandably, about the fact that we have to be realistic and we cannot do it all. And then you listed the five buckets, some of which imply

an intensity of threat, seriousness of threat, and a lot of which understandably are priorities of methods for combating threats.

So I wanted to ask you, as we look forward to the next 5 years, if you could address the question of risk in a somewhat different manner, which is what you believe the biggest security risks are that America will face here at home, and let's focus for a moment at first on terrorism. Obviously, we face the continuing threat of a natural disaster like Hurricane Katrina, but I am thinking about the terrorists. As you order the ways in which terrorists may attempt to attack us, what is the priority list?

Secretary CHERTOFF. Risk is composed of three things: Threat, vulnerability, and consequence. And, frankly, I put the most weight on consequence because threat and vulnerability change, consequence rarely does.

The high-consequence event that is the biggest risk is a weapon of mass destruction. A nuclear bomb, of course, is at the end of the scale. A biological attack, even a serious radiological attack, would have very powerful effects on our entire country.

The good news is at least in terms of a nuclear bomb, the likelihood of that happening, the threat in terms of capability, is low at this point. On the other hand, I have no reason to believe that threat is going to diminish over time, and I do have reason to believe it is going to increase over time.

Senator LIEBERMAN. So would you put that at the top of the list?

Secretary CHERTOFF. I would put that at the top particularly because we need to be making the investments now against the day 5 years from now when that threat does become more likely.

Senator LIEBERMAN. And the investments are in prevention or response?

Secretary CHERTOFF. Well, they have got to be in everything, but I have to say with a nuclear bomb, prevention has to come first because there is no way a response to a nuclear attack is going to be anything but inadequate in terms of the lives lost and the damage done.

Senator LIEBERMAN. Right. So let me ask you to take a moment and now relate your five buckets to what you have stated is the number one terrorist concern you would have, which is a WMD attack, particularly a nuclear attack. How do we prevent it?

Secretary CHERTOFF. Screening bad things out. A critical element of what we have to do is keep out dangerous things from the country, and that is why I put radioactive material at the top of the list.

Now, that has to begin, as Senator Levin said, overseas. The President signed an agreement with President Putin during the G–8 to be much more aggressive in terms of our overseas efforts to intercept this material.

From the homeland standpoint, eventually we want to make sure that even before a container is loaded into a ship, we are screening it for the possibility of radioactive material. We also, by the way, will have by the end of next year radiation portal monitors at each of our land ports of entry.

Senator LIEBERMAN. Right.

Secretary CHERTOFF. So that ring around the country is step one.

Step two is what we call the "Securing the Cities Initiative." We anticipate over the next 2 years putting money into and deploying

radiation detection systems around at least one major city, the city of New York, and two other cities yet to be selected, the idea being that we will then build on that to have a network of radiation detection equipment inside the country itself. So that is one bucket.

Another bucket is intelligence. The DNI, Ambassador Negroponte, is very focused on counterproliferation. Much of our collection activity is aimed at determining whether there are people out there building the capabilities to develop nuclear weapons.

Senator LIEBERMAN. Right.

Secretary CHERTOFF. So enhancing that is a second issue.

A third issue is response, and whether it be a radiological bomb or it be a biological attack, we have to have the capability to come up with an antidote or a vaccine. And the good news is with respect to many of these threats, we have the antidote. We also need to be able to distribute it, and much of the planning that we see, for example, in the avian flu area is also a way of planning for how we would do a mass distribution with respect to other kinds of biological vectors.

I can also tell you that we have deployed in a significant number of cities biological detection equipment which goes off when there is an ambient indication of a biological measure because that enables us to respond more quickly.

So those are three areas in which we respond to that high-consequence event.

Senator LIEBERMAN. How about the prevention of the movement of chemical and biological materials into the country in place for an attack? In other words, we are focused, understandably, on trying to detect the coming of a nuclear weapon. I understand this is different because you could put together chemical and biological means for an attack within the United States. What systems do we have to prevent that? Intelligence obviously is one. If we can know what is coming and break it before it gets here, that obviously is the best way to do it.

Secretary CHERTOFF. I think the challenge with biological and chemical is that there is plenty of stuff inside the country. You do not need to bring it in.

Senator LIEBERMAN. Yes.

Secretary CHERTOFF. And we saw in the Oklahoma City bombing that ammonium nitrate could be a powerful weapon.

Now, we do regulate, particularly with respect to biological hazards, we do some regulation with respect to the way in which it is made available to the public. But there are some kinds of chemicals and some kinds of biological agents that occur in nature, and if someone had the wherewithal, they could simply take something that occurs on a farm, like anthrax on a farm or foot-and-mouth disease on a farm, and they could, if they had the know-how, culture it to make it weaponized.

So there the focus has got to be—we cannot keep it out of the country. We have got to focus on intelligence. We have got to focus on rapid detection capability so that if there is an outbreak, we can move quickly in order to tamp it down. And that is an area, frankly, where our ability to distribute vaccines or antidotes quickly is really our principal method of defense.

Senator LIEBERMAN. OK. My time is up. So, clearly, the No. 1 threat is a weapon of mass destruction.

Secretary CHERTOFF. In terms of consequence.

Senator LIEBERMAN. Chemical, biological, or nuclear, in terms of consequences. I would like to come back, unless someone else asks you about it, how you rate—and I won't ask you for an answer now—the threat of an improvised explosive device here. Obviously, these are being used elsewhere around the world by terrorists.

Thanks from your answer, and it guides us in prioritizing our own work with you to try to prevent and protect and respond to that number one concern that you have. Thank you.

Chairman COLLINS. Thank you. Senator Coleman.

Senator COLEMAN. Thank you, Madam Chairman.

I want to follow up on Senator Lieberman's questioning about the No. 1 threat being a nuclear weapon, nuclear material, and the ability to bring it in through cargo, through our ports. I think we deal with about 11 million containers entering the country every year, and we have had discussions—and I appreciate your taking the personal effort, Mr. Secretary, to go to Hong Kong to take a look at that system.

One of the nice things about this Committee with the leadership of the Chairman and the Ranking Member is I think we have done a pretty good job putting partisan politics aside and trying to figure out what is the best thing to do. And I am a bit concerned with the politicization of kind of the fear of something getting in there. The *Washington Post* has an editorial today where they talk about mandating 100 percent screening, and they use the phrase, "The 'inspect all containers' mantra is a red herring that exploits Americans' fears about what might slip through in order to score political points . . . "

Let me talk to you a little bit about that. The screening of nuclear radiation that you talk about, 100 percent, that is in our country, those are in our ports.

Secretary CHERTOFF. Correct. And I want to be careful to use the word "scanning" because what we do is we put them through scanners, and that is in our ports.

Senator COLEMAN. All right. But the ideal situation, of course, is to get them outside because clearly if a device comes in and it were to be in Long Beach, New York, or Savannah, wherever it is, New Jersey, it would have a devastating impact on not just people but commerce, and it would be very disruptive. So ideally we want to do the screening out, and then set up—we have our CSI, Container Security Initiative. We have the pilot project looking at the Hong Kong system. But Hong Kong, as you and I know, Mr. Secretary—I think it is two lanes out of 40 that does 100 percent. And now there are proposals that say we need to do all cargo within 3 years or 4 years.

Can you respond? Again, I want to push you on this really hard, but tell us what is it that we can do, and even on an accelerated pace, what can we accomplish in this area?

Secretary CHERTOFF. I think, first of all, the biggest constraint—there are two constraints on our ability to operate overseas. One is, of course, there has to be enough physical room to put these devices in place without significantly slowing up the flow of the con-

tainers. And I think you are quite right, Senator, in pointing out that each port is going to be different, and their capacity to manage the throughput is going to depend on the nature of the port.

The second issue, frankly, is the willingness of foreign governments to cooperate, which we do not control, because when containers go through the system that we are proposing to start to deploy, when they hit a red light, some of the containers have got to be pulled out and have got to be opened. You have got to inspect it. And the authority to do that lies with foreign governments. We work with them, but it is their authority that we use to open the containers.

They rightly worry about the burden on their own customs officials in terms of whether they have the manpower and the capacity to do that. So I cannot tell you that within 3 or 4 years we can fully deploy a system of having everything, every container overseas go through a dual scanning system before it gets on a ship because I cannot predict that foreign governments will agree, I cannot predict that every port is going to be configured in a way to allow that to happen. And I would hate to have Congress pass something that would suggest to the American people that there is a solution that is completely pie in the sky.

Senator COLEMAN. But we can tell the American people that every single container—every single container—is undergoing a review process.

Secretary CHERTOFF. That is correct. Every single container is screened in two ways.

First of all, based on information that we obtain about the shipper, the track record, the destination, method of payment, and a host of other considerations, and then the high-risk containers are physically inspected or run through X-ray machines.

Second, by the end of next year, all containers, once they—at least at the point they arrive at our ports, will be taken through radiation portal monitors before they leave the port. So while not a perfect defense, it is a very good defense.

Senator COLEMAN. And I keep going back to the former mayor in me—and I think we have a number on this panel. There was not a partisan way to collect garbage, I just wanted to get it done. And I am not going to be satisfied—if foreign countries are not cooperating, then we need to do something about that. That is not an acceptable excuse for me. Then we need to say that they are going to have some consequences. But I just want to make sure that we do not get caught up and this become a political football. It is too important an issue. And we will push you, Mr. Secretary. We do want to see the results of the Hong Kong project. Clearly, one of the challenges of Hong Kong is that information right now is not integrated into the full system. So we have got a lot of data there, but it is not being used currently. And so the challenge first becomes to use it, to have it integrated into our system, and then to assure the American people that, yes, each and every container is being reviewed and that we are maximizing and pushing to the limit of making sure what we can physically look at without in the end doing what Osama bin Laden wanted to do, which is to destroy our economy.

Thank you, Madam Chairman.

Chairman COLLINS. Thank you. Senator Levin.

Senator LEVIN. Thank you, Madam Chairman.

I want to talk to you about the watchlist, Mr. Secretary. The Terrorist Screening Center was supposed to have developed a system through which screening agencies could directly access the database, but this has yet to be completed. That is what the GAO says. Is that correct?

Secretary CHERTOFF. I can tell you what my understanding is. There is a no-fly list that is compiled from individual databases maintained by individual agencies, and that list is accessible as a single list or as a single database, and that is what keeps people off of airplanes.

At the border, there are a number of different databases because different agencies keep information for different purposes, but it is possible to access them all immediately from the port of entry so that we are capable at our ports of entry of screening a list within a matter of moments for somebody coming——

Senator LEVIN. How many lists are there?

Secretary CHERTOFF. I don't know if I can give you an answer to that. Probably somewhere between half a dozen and 10, depending on how you want to characterize them.

Senator LEVIN. Let's say a half a dozen. Why aren't they integrated into one watchlist?

Secretary CHERTOFF. I think two reasons. First of all, there is actually no reason to make them a single list, and there are reasons not to make them a single list. The reason we do not need to make it a single list is in this day and age it is possible to check a name against four or five lists simultaneously, with very little loss of time. I mean, it is all done in a matter of seconds.

The downside with merging them, as opposed to integrating them, is that they are held for different purposes. For example, the FBI has lists of people who are involved with criminal behavior or dangerous behavior, which includes American citizens. But that is not really of use to the Border Patrol in its entirety because we cannot keep American citizens out of the country. They have a right to come in. And, in fact, privacy advocates generally argue that unnecessarily merging lists into one actually raises the risk to privacy.

Senator LEVIN. Can a local law enforcement person who arrests someone who wants to see if he is on any terrorist list access immediately all of the lists?

Secretary CHERTOFF. We have now completed phase one of merging IDENT and IAFIS, which are the two fingerprint-based systems, our system and the FBI's system, and I believe in Boston and some other cities, we are now deploying that kind of inter——

Senator LEVIN. But that local law enforcement person out there in most jurisdictions cannot right now access, after they arrest somebody, all of the terrorist watchlists?

Secretary CHERTOFF. I think that is right. I think they can get the information that is pertinent to them through one of two portals—either the FBI portal or through this merged portal that we are beginning to deploy.

Senator LEVIN. So that a law enforcement person who arrests somebody or is suspicious of someone can, through two portals,

punch a button, get all the information that all the agencies have that would make this person a suspicious character——

Secretary CHERTOFF. I don't know if I can make it "punch a button." But in whatever way they access, for example, IAFIS, which is the Bureau list, they can access that, and through this new program, we are making it available now in some areas because we have now begun phase one of merging these two.

Senator LEVIN. So that is not yet available in most place?

Secretary CHERTOFF. It is not yet fully available, correct.

Senator LEVIN. All right. Do we have all the resources to make it available?

Secretary CHERTOFF. I think the issue is not a money issue. I think it is a systems issue, making sure that we can deploy it in a way that is not going to create false positives. I think we are going to watch phase one, and I think we are on track to completing the job in short order.

Senator LEVIN. Because I think when you just testified that we have a unified watchlist and we have an integrated watchlist, it makes it sound a lot more advanced than it really is.

Secretary CHERTOFF. Well, I want to be clear. I was particularly being—I want to focus on, first of all, the TSA no-fly list because there seemed—I was reading things in the paper today that were suggesting that we do not have a unified no-fly list, and I can tell you that is incorrect.

Senator LEVIN. That is not what I was referring to, though. Let me ask quickly because I only have a minute and a half left. How many of the people who were arrested in Britain had visas to the United States?

Secretary CHERTOFF. Britain does not—under our Visa Waiver Program, if you are coming as a tourist, you do not need to have a visa to come from the United Kingdom or a couple dozen other countries in Europe.

Senator LEVIN. So that many of those people had tickets to come to the United States?

Secretary CHERTOFF. If they were coming—yes, they had tickets—well, I would not say many had tickets, and I want to be careful about not saying things that are going to create a problem for the British case. I don't think they had tickets yet, but I think they could have acquired tickets and would not have needed visas if they were coming in, allegedly coming in as tourists.

Senator LEVIN. Now, had the British that had been following some of those people for a long time notified us of that fact so that they would not get tickets to come to the United States?

Secretary CHERTOFF. We were made aware in timely fashion of the identities of the people. We would have prevented them from getting on planes.

Senator LEVIN. From getting tickets?

Secretary CHERTOFF. I don't know if we would have stopped them getting tickets. They would not have gotten on airplanes.

Senator LEVIN. All right. So that we have checked through all these people and we know that we would have stopped them from getting on airplanes?

Secretary CHERTOFF. Yes, because we would have had their names.

Senator LEVIN. We did have their names?

Secretary CHERTOFF. Correct. Well, we had the names of many of them. I mean, there may have been some that turned up in the course of the investigation once the arrests started to get made.

Senator LEVIN. No, but I mean before that part of the investigation——

Secretary CHERTOFF. The people that they——

Senator LEVIN [continuing]. Began, we had all the names that the British had.

Secretary CHERTOFF. Correct.

Senator LEVIN. OK.

Secretary CHERTOFF. Yes.

Senator LEVIN. Finally, what percentage of State or local first responders would you estimate now have truly interoperable communications equipment so that they can communicate with State, local, or Federal agencies? Just give us a rough perspective.

Secretary CHERTOFF. I know the 10 largest cities through our Rapid Command Program have what we would call command-level interoperability, which means that the agencies and jurisdictions in the region can talk to one another at the command level.

I cannot estimate for you in other parts of the country because I think a lot of it depends on whether they have purchased this gateway equipment, and a lot of it, frankly, depends on whether they have built the rules that will allow them to talk to one another.

However, by the end of this year, we will complete a study and a survey of the 50 States and the 75 largest urban areas precisely to ask them to test what their interoperability is and then to come back and tell us what the gaps are.

Senator LEVIN. Again, I share what others have said here with you that this is the greatest single complaint, I believe, that we get from local first responders and law enforcement people—the shortage of interoperable equipment. And it is not just because they have not worked out the ground rules with other jurisdictions. There are many cases that I know of where applications have been filed for funding where those ground rules have been agreed upon, and yet the funding has not been forthcoming. So I do not think that is an adequate response to a lack, an obvious lack of interoperable equipment where there is a good reason to have interoperable equipment and the ground rules have been worked out. And I hope you will pay some additional attention to that issue.

Secretary CHERTOFF. I will. And when this survey is completed, if it turns out, for example, that you have a jurisdiction where they have the ground rules and they do not have the equipment, we have grant funding available, which we will be pleased to make available to get that equipment.

Senator LEVIN. Well, it is inadequate, I can assure you. Thank you. Thank you, Madam Chairman.

Chairman COLLINS. Senator Voinovich.

Senator VOINOVICH. Yesterday I had a meeting with the Jewish community in Cleveland, and it brought home to me something that I have been concerned about for a long time, and that is the radicalization of our own Muslim population here in the United States.

I just completed a book by Gilles Kepel called "The War for Muslim Minds." We have got to recognize that this is a different war than we have had before. It has a lot to do with the minds of individuals and how do you deal with modernity and how do you make sure that you do not have homegrown situations.

What I would like to know is: What is being done on the Federal level to develop the infrastructure of understanding and human relations in communities around the United States of America to get people together to talk to each other so that we do not end up with Muslim xenophobia and folks that heretofore have felt integrated in a society feeling that they are not part of our society? Kepel in his book says that he believes that one of the ways that we need to be successful in Western nations is considering how we deal with integrating Muslims into our societies. In some countries it has been very effective, in others it has not been so good. But what is going on at the Federal level? Mr. Secretary, whose job is that? Yours? Karen Hughes'? State Department's?

Secretary CHERTOFF. Well, I think it began with the President saying shortly after September 11 that this was not an attack by Muslims and that we should not allow this to draw us into characterizing Muslims or people from certain parts of the world as being anti-American, that it was an attack by a number of ideologues who happened to use the language of Islam.

It is a shared responsibility in this sense: I mean, we are doing a lot of work, some with the academic community, trying to understand the psychology of radicalization and trying to understand why it is, for example, that there are problems in Western Europe that we have not yet had, some of which flow from the nature of the societies over there. Part of it is simply getting out there and interacting. I mean, I have tried on a number of occasions to go out to the Muslim community or have them come meet with me to interact with them and speak with them. Part of it is recruiting and encouraging Muslim Americans to become part of doing public service and working in law enforcement and working in intelligence. And we have some of them.

We all recognize that people of all ethnic groups can be involved in criminality or terrorism, and it does not condemn the ethnic group. What we have got to do is continue to build upon those positive aspects of our society that make people——

Senator VOINOVICH. Well, there is certainly a Federal aspect to this, but I also think the infrastructure of understanding and human relations is largely built at the local level.

Secretary CHERTOFF. It is community-based.

Senator VOINOVICH. It is. When I was mayor of Cleveland, we had significant tension between our minority community and our police department. So we started a dialogue to bring people together to talk about it; to enhance communication and build ties. And I am really concerned that at the national level, there is not any real thought being given to how to work with maybe the National League of Cities or the U.S. Conference of Mayors to try to get the cities to start to think about how to bring people together on this issue. How do we reach out to the top Muslim leaders in the United States, identify who they are, begin to have a real dialogue with them, and also include the Jewish community?

My other concern on an international level is the Organization for Security and Cooperation in Europe. For 4 years, I have been trying to get them to make anti-Semitism and Muslim xenophobia priorities because that is the underpinning of many of the tensions in communities. And I think so often what we are doing is preventative, to make sure something does not happen. But I think outreach is equally important, and how successful we are going to be will depend upon how well we start to work at integrating our American Muslim community.

Secretary CHERTOFF. Well, I agree with you. Certainly internationally, Under Secretary Hughes is very focused on this. I know the President is actually focused on this. And, domestically, as I say, as we do this research, I think it is a very good idea for us to get some of the perspective we accumulate out to the cities and the States through the various organizations like the NGA and the National League of Cities because, I agree, the front line on understanding does lie in the local community.

Senator VOINOVICH. Well, I would like to work with you on that.

The other thing, and this is a big issue, as you know, we have been monitoring DHS management in my Oversight of Government Management Subcommittee, and I want you to know that I am deeply concerned about the high level of staff turnover and vacancies at the Department. This is a particularly serious problem at the senior leadership levels. The Committee has been aware of vacancies at FEMA. We know about that, Madam Chairman. But there are also continued vacancies in the Transportation Security Agency, Immigration and Customs Enforcement, Customs and Border Patrol, and the National Cybersecurity Division.

What are you doing about filling those vacancies? Also, is there a long-term strategic management plan in place about what needs to be done in the agency? And how long is it going to take to get it done?

Secretary CHERTOFF. Let me answer both parts of that. The issue with respect to turnover is twofold. It is not, by the way, restricted to DHS. I mean, the Bureau, the FBI, has had a significant amount of turnover in the counterterror area. And I will be blunt. It is a hard job. After 3 years, people get burned out. They get tired. And, frankly, there is not a lot of patting on the back, and that tends to drive people out of the agency, too.

I wish I could hold these people—there are people—I mean, sometimes you want to see people go, but sometimes there are people you do not want to see go. But you do not have the ability, when people get really tired out, to look them in the eye and say, "You have got to keep going." It is a real sacrifice for some of these jobs.

We are working very hard to fill these jobs, and we have been successful in doing it. It is a cumbersome process. I have been particularly frustrated with the ability to fill the cybersecurity job. It is hard to compete with the private sector. I cannot pay nearly the amount of money you can make in Silicon Valley. On top of that, we have laborious and sometimes unpleasant background checks, requirements of financial divestiture that people sometimes finally say, "I cannot be considered because I am going to be sacrificing the ability to put my kids through college."

So we have been very lucky in that the number of public-spirited people of top talent who we have gotten to join the agency during my tenure is extraordinary. We have had people like Charlie Allen and Kip Hawley and George Foresman. There are other people I would like to consider, but it is hard to recruit. We are continuing to work on that.

On the larger management issue, we do have a strategy to implement this kind of a strategic plan for completing the integration, which involves not only merging the number of IT systems into a single system, finishing the job of having our financial systems reduced in number, empowering the chiefs of the various business lines to have more authority over their counterparts in the individual components, but also bringing a career path into fruition that, much as DOD does, actually rewards you for activities that are either joint or undertaken with other agencies and that has an educational process for the senior leadership that will emphasize that, like the Capstone or Pinnacle program at the Defense Department.

I have asked my Deputy actually to work on this, and I am envisioning he may come sit with you and give you a little bit more granularity about that.

Senator VOINOVICH. Thank you.

Chairman COLLINS. Senator Dayton.

Senator DAYTON. Thank you, Madam Chairman. I would also like to join with others who have complimented you and the Ranking Member, Senator Lieberman, for your leadership on this and holding this very important hearing.

Mr. Secretary, I need to, I guess, respectfully disagree with what I took to be your presumption that the American people are not willing to pay for or we have to posit a choice between bankruptcy and the maximum necessary homeland security. I think if you posit to the American people do you want realism as defined by, at least in Minnesota, a 60-percent reduction in funding for its homeland security plan from a year ago, people would say, I think almost overwhelmingly, if not unanimously, they do not want that kind of less-than-adequate funding. And it is hard to assess from the Legislative Branch what is sufficiency in funding. That is where we really have to defer to you. But I worry that the Office of Management and Budget is defining our funding commitment to homeland security rather than your or rather than what the imperative is.

Again, having witnessed firsthand the last month, both the Southern border effort and certainly the Northern border, I think it is inadequate. I think while certainly progress has been made, that progress is insufficient to the risks involved. And, again, I think the American people expect from us—not perfection, that is impossible, but they expect from us that we are going to be doing everything that is feasible as rapidly as feasible in order to provide the maximum optimal homeland security; and if we are not doing that, I think we need to be candid with one another, you and Congress, and then with the American people, why it is we are not fiscally capable of undertaking that kind of priority.

Secretary CHERTOFF. Well, I agree with you it has to be optimal, but I think there are several different realities we have to recognize. One is you could in theory spend a limitless amount of money

on security. People can do that in their own home. I mean, I could redo my house and buy five locks and buy steel doors and buy expensive security systems with sensors. There is always more you could do. We all make judgments about what the optimal amount is.

But it is not just a question of spending money. We cannot put into effect systems that destroy our ability to operate in our way of life. I mean, I could give you—a perfect example is the issue of getting on the airplane. Some people argue we should ban all hand luggage, walk on with nothing in your hands, not even a magazine. That would clearly increase security. There would be a high cost to people in doing that—not a monetary cost but a personal cost. Business travelers would find it very difficult. Mothers would find it difficult.

So what we wind up doing is we wind up balancing. We wind up looking at what is the marginal additional benefit and what can we accomplish without requiring that sacrifice.

We are going to have disagreements about that. Even those who are experts have disagreements. But I think the principle that there are limits and balance I think is when we disserve the American people if we don't emphasize that we are always facing choices.

Senator DAYTON. I respect that. I am glad you went to Hong Kong. I mean this sincerely. I would prefer you come to northern Minnesota and talk with especially the local law enforcement officials there and get their perception of what—I think the imbalance, at least as it exists up there, is decidedly on the side of lack of sufficiency rather than the excess, which I agree with you, more is never enough.

Regarding the interoperability issue, and I am way beyond my limited expertise when you talk about something like gateways, but that is a problem, again, with the local officials in Minnesota. You talk about leadership. If there is an expertise that your agency possesses about how to define this—because I think it is critical, as you say, that people get on the same page before they are spending money to upgrade their equipment or buy new equipment and compound the problem rather than resolve it, whether there is some kind of national conference or State conferences that you could be part of—your agency be part of either convening or participating in, I certainly, again, would like to convene one of those in Minnesota because I think the local officials are starving for that kind of understanding, if they do not have it, if it exists out there, that expertise, they do not have it. And I think to communicate that now, as I say, before we are spending more money that is not going to resolve the problem or make it worse, it would really be imperative.

Secretary CHERTOFF. Well, that is why we are doing this study with the States in the 75 large urban areas, precisely to pinpoint in a systematic way what the gaps are. And once we get that done by the end of the year, I think we can have a much more focused discussion with the States and localities about what it is they really need and what it is they have to do in order to get up to snuff.

Senator DAYTON. Well, I think the time, the urgency of that undertaking, if it needs to wait until the end of the year until the

study is complete, but I hope the beginning of next year then your agency could provide that leadership and that expertise and get everybody as much as possible, at least show them what the page is. If they are not going to get on it, that is their responsibility, but at least give them that guidance.

Thank you, Madam Chairman.

Chairman COLLINS. Thank you. Senator Bennett.

Senator BENNETT. Thank you, Madam Chairman.

Mr. Secretary, I have to say I am impressed at your presentation here this morning, the degree to which you have gotten your arms around the problems and catalogued them in a way that is very coherent and intelligent. And I come away from the hearing with a higher sense of confidence in the level of progress that has been made by the Department. We both understand it is not where it wants to be, where it needs to be, but frankly, in the period of your stewardship, it has moved farther than I might have anticipated that it would.

Most of the concerns that I have had have been talked about by those who have questioned you before me, but I want to come back to Senator Voinovich's question and focus on one aspect, which you raised in your response to Senator Voinovich, and that is the Assistant Secretary for Cybersecurity and Telecommunications. You may remember that I got quite exercised about that and urged you to move ahead and was delighted when it was created. Now it has been a year since that position was created, and it still has not been filled.

And I hear what you said to Senator Voinovich about the difficulty of filling it, but I want to share with you my own experience when I have been to Silicon Valley, where the first question I was asked was, "Why hasn't this position been filled?" And my answer was not as completely sophisticated as yours, but it was basically the same answer: "Well, Federal salaries compared to Silicon Valley salaries are so low that they are having a hard time attracting somebody." And I was told, "Senator, we will give you a list of half a dozen people who are willing today to give up their Silicon Valley salaries to come into government service on a 1-year, 2-year kind of mission, if you will, to try to get that thing under control."

I don't know if you have been to Silicon Valley. They did not give me the list, so I have no names to share with you. But have you made that kind of an effort to say, "All right, we understand that this is a fairly significant financial sacrifice on your part, but your country needs you and give us 2 years, step aside from your more highly paid job, step aside from your career long enough to sacrifice for your country," and gotten any kind of a response?

Secretary CHERTOFF. I have been to Silicon Valley, Senator, and first of all, I want to say that I believe we will actually be in a position where the President will have somebody to nominate in the very near future. But I actually tried to do some of that and also reached out through people in the Department who have backgrounds working with people in the field. I want to be careful not to get specific about people in a way that would invade their privacy.

I would say that it was a combination of challenges. It has really been probably the biggest personnel frustration I have had since

taking this job because I have had extraordinary people coming to fill other jobs. This one, it has been a combination of not just the money, but many of the people with experience face conflict-of-interest issues because the technology they would have to pass upon would have been technology that they had something to do with, or they have divestiture issues, which I frankly—it is hard to argue to people—or it is one thing to give up your salary. It is another thing to get into a hefty divestiture, particularly if you are a comparatively young person. And some of them eventually just culturally were—took themselves out of the running. We had some false starts, I would say.

I think we are at the point now where I am hopeful we will have this position filled in very short order, but I confess to you that filling this job has been really tough.

Senator BENNETT. I understand that, and it may be, Madam Chairman, Senator Lieberman, that Senator Voinovich with his interest on human capital, we consider amendments to the law that say for a specified period of time—that is, if you serve for a specific period rather than make a career, there can be a waiver for some of the other aspects that you have. In my position as Chairman of the Agriculture Subcommittee of Appropriations, we run into some of this same sort of thing with respect to the FDA because the rules are very firm that you cannot be an expert for the FDA if you have any connection with this, that, or the other pharmaceutical company. And we end up unable to draw on anybody who has any real expertise because everybody who has an expertise has someone who is willing to pay for it. And we take the automatic assumption that if someone on the outside is willing to pay for your expertise, you are prima facie corrupt and, therefore, cannot work for the government.

Now, I do not believe that is true. This is as critical a position in Homeland Security, as I think Secretary Chertoff has made clear, as we can find, and perhaps we ought to consider in this area, and maybe some others, passing legislation that would say if they come in for a specific period of time, they are not going to be in a permanent situation, they ought to be allowed a waiver from some of these conflict-of-interest circumstances, as long as they are fully disclosed and everybody understands all of them, because failure to do that leaves us naked in an area that, if I were a terrorist, would be my first area of attack on the United States right now.

I think we could have greater devastation shutting down some computers, hacking into the capacity—talk about interoperability of equipment. If you hack into the network that these people are using and shut the network down, the equipment could be the best in the world and it does not work. And having someone focusing on this with the kind of attention that it needs is very critical, and we have gone, frankly, longer than we should have to create the position, and now we have gone a year without anybody in the position. And I think it is something that Congress ought to look at because I believe the Secretary has laid out his challenge very dramatically to us here this morning.

Chairman COLLINS. Thank you. Senator Lautenberg.

OPENING STATEMENT OF SENATOR LAUTENBERG

Senator LAUTENBERG. Thank you very much, Madam Chairman.

Mr. Secretary, I commend you for the effort and the intelligence that you bring to this assignment. It is still such an incredibly complicated, gigantic thing that I think that despite your efforts and a lot of interest in what is taking place, there is still some exposure that we ought to try to deal with as quickly as we can.

Do you believe that 100 percent inspection of cargo would be a worthwhile endeavor?

Secretary CHERTOFF. I want to define three separate things: "Screening," which means identifying through intelligence and information what is in the cargo, we do 100 percent. "Scanning," running through radiation portal detection equipment, we will be close to 100 percent by the end of next year. "Physical inspection"——

Senator LAUTENBERG. It currently is 5 percent.

Secretary CHERTOFF. No. Running through radiation——

Senator LAUTENBERG. Scanning?

Secretary CHERTOFF. Scanning through radiation portal monitors in our ports will be 80 percent by the end of the year and close to 100 percent by the end of next——

Senator LAUTENBERG. In our ports. Are you talking about cargo containers coming here——

Secretary CHERTOFF. Correct.

Senator LAUTENBERG [continuing]. Will have already been scanned——

Secretary CHERTOFF. No. When they arrive, before they leave the port, they will have been scanned through radiation portal monitors, 80 percent will have been scanned—we will be at 80 percent by the end of this year and close to 100 percent by the end of next year.

Senator LAUTENBERG. This is after the container has been put down on American soil.

Secretary CHERTOFF. Correct. That is correct.

Senator LAUTENBERG. And if there is something in there that is designed to wreak havoc in our community, would it be a little late? It takes some time to get the cargo off the boat and——

Secretary CHERTOFF. Well, the screening, in terms of intelligence-based screening, in terms of what is in the container, is something we do—actually a good deal of it we do overseas.

Senator LAUTENBERG. Yes, I would like to pass that, if you do not mind, because screening to me is not really an effective way to do it, and I particularly want to focus on the scan side.

Secretary CHERTOFF. The scanning, some of it we do overseas, but the vast majority of it is done once it has arrived here. That is why, as I said earlier, I went to Hong Kong, we looked at the system they have there, and we are——

Senator LAUTENBERG. When did you go, Mr. Secretary?

Secretary CHERTOFF. This spring. I think it was March or April.

Senator LAUTENBERG. This year.

Secretary CHERTOFF. And we are working with a number of foreign governments now to begin to deploy a system overseas that would scan containers before they actually get loaded on the ship. The constraint there, as I said earlier, will be twofold: It will be making sure that physically they are able to do it, given the con-

figuration of the port; and, second, of course, the foreign government has to agree because it is their port.

Senator LAUTENBERG. Do you believe that it can be done? The equipment that you saw in Hong Kong, does it work as it is suggested, a 2-minute slide-through and a relatively modest cost per container?

Secretary CHERTOFF. I think it moves quickly, but there are some technological barriers. One of them is, depending on the nature of the port, sometimes there is background radiation that creates a problem. And the second thing is you have to have the ability, when you actually do get a red flag, to do a timely inspection. The constraint there is whether the foreign port has enough inspectors——

Senator LAUTENBERG. I am going to interrupt you, as much as I hate to do it, because we were friends way before we got here. So would it make us safer in any measure, do you think, scanning the cargo?

Secretary CHERTOFF. Overseas?

Senator LAUTENBERG. Yes.

Secretary CHERTOFF. Sure, I mean, if we can get it done in practical terms and if the foreign governments are supportive, that is where we would like to go.

Senator LAUTENBERG. Would you think that it is an appealing idea—scanning each of 11 million cargo containers entering American ports each year is a recipe for crippling our manufacturing and commerce, wasting time and money that could be better used for other measures, adding little to our homeland security? Do you agree with that statement?

Secretary CHERTOFF. I want to be real careful because people use words in different ways. I think the idea that you are going to physically inspect every container is not realistic and would, in fact, destroy the entirety of our maritime system. I think the ability——

Senator LAUTENBERG. Would a nuclear explosion in a cargo container destroy our maritime system?

Secretary CHERTOFF. It would, Senator, but you could also bring a nuclear container through a container on the back of a truck coming from Canada. So the logic——

Senator LAUTENBERG. So what do we do? Do we just throw up our hands——

Secretary CHERTOFF. No.

Senator LAUTENBERG [continuing]. And say because that could happen, why bother?

Secretary CHERTOFF. No. Again, what we try to do is we try to come up with a risk-based solution, one that raises a significant barrier to the risk, but not at the cost of destroying that which we are trying to protect.

I think that a combination of what we are doing with radiation scanning here, what we are working with foreign governments to do overseas—and I would love to see us do this Hong Kong pilot, roll this out overseas, and we are going to be doing that over the next few years—I think that is all good, and that will really raise the barrier. I do think that 100 percent physical opening is not realistic.

Senator LAUTENBERG. Well, not opening, but, again, scanning, if you are looking for radiation, if you are looking for explosive materials, and that can be detected promptly.

I read further from a press report that was handed out by this Committee during a press conference before in which it declares that 100 percent scanning of cargo containers is a red herring, and we say—it says, "Even if manpower and equipment necessary for 100 percent scanning were available, the process would impose delays and create massive backlogs at ports. Scanning a shipping container takes several minutes. Analyzing the scan images can take up to 15 minutes." Is that correct?

Secretary CHERTOFF. I think, Senator, it is going to depend a lot on a number of different things. It is going to depend on whether it is a transshipment port, which means you have containers coming from Port A to Port B, and then they have to be offloaded—that makes it much more difficult and time-consuming—as opposed to a port where the containers originate in the port and, therefore, they just move through in a single line. It depends on the physical structure of the port.

Senator LAUTENBERG. But it does not necessarily—you are not suggesting that it does simply impose delays, create massive backlogs at ports? I mean, do you see our industry and our economic activity being destroyed by scanning, attempting to scan 100 percent of the cargo that comes in?

Secretary CHERTOFF. I understand, Senator, you are trying to drive me to give you a yes or no answer.

Senator LAUTENBERG. Yes, I would like that.

Secretary CHERTOFF. If I am going to be accurate, I cannot do it. I have got to tell you it depends a lot on the individual port. In some ports, we are probably going to be able to do something like 100 percent scanning overseas, and we are working to see whether we can get some ports in the next couple of years to——

Senator LAUTENBERG. I am going to be cut off here very soon, but there is a bill on the floor of the Senate in which I called for 100 percent scanning of containers and am attempting to get that done. The Committee has in turn decided that three pilot projects would be enough.

Mr. Secretary, you and I were at a very important event yesterday with citizens typically from our State of New Jersey, your State and my State, 700 people died; there still is injury that affects the health and well-being of people. A firefighter died last week who tried to help in the rescue operation because of a lung disease that he contracted.

So when we talk to those people, we make promises that we are going to do everything we can to try to keep them safe. And to me, when we start talking about pilots when, in fact, we have effective equipment—you say the equipment is effective in Hong Kong that you saw?

Secretary CHERTOFF. I mean, the pilot was effective, but I have to qualify it. There were some constraints in the ability to use it in real life, and that is what I do not want to do is tell the American public we have got a magic bullet and the bullet turns out not to be effective. So, I mean—there is promise in——

Senator LAUTENBERG. So the alternative to that is tell the public we are going to ask you to take some more risk while we pursue this debate.

Secretary CHERTOFF. Senator, I can say this because we are old friends. I confront this argument a lot, and there is nothing I would like more than to be able to say, Wow, we have a way to make every port in the world scan all the radiation overseas. But I cannot do that with a straight face because not every port is physically constructed to be able to do that, and not every country is willing to do that, and I cannot make other countries do things.

It is like I get in my car or I put my daughter in my car, I understand it is not 100 percent safe. If I wanted my daughter to be 100 percent safe, I would put a 5-mile-an-hour speed limit cap on the car, and it would not go more than 5 miles an hour. But I do not do that because that is more safety than we can afford.

All of us—we have 40,000 people die every year on the highway. That is a guaranteed 40,000 who die. We do not require that cars be manufactured to go no more than 5 miles an hour. So we do judge this——

Senator LAUTENBERG. But we require them to be sober and we have red lights and we have other things.

Secretary CHERTOFF. That is right.

Senator LAUTENBERG. We have other protections, and if we——

Chairman COLLINS. The Senator's time has more than expired.

Senator LAUTENBERG. And if we inspected one out of 20 people going into the White House for tours or coming into this place, would we feel secure? I don't think so.

Thank you very much, Madam Chairman.

Chairman COLLINS. Senator Carper.

Senator CARPER. Thanks, Madam Chairman, and thank you very much for your testimony, Mr. Secretary, and for your responses to our questions.

I want to come back to a point that you made with respect to chemical security, an issue that this Committee spent a whole lot of time on, and with the leadership of our Chairman and Ranking Member, we hammered out a consensus, at least on the surface, and reported a bill out—I don't know, was it unanimously or——

Chairman COLLINS. Unanimously.

Senator CARPER. Unanimously, which was a minor miracle, as I recall, a month or two ago.

Senator LIEBERMAN. A major miracle.

Senator CARPER. There you go.

There are those who—and I know Senator Lautenberg spent a lot of time on this. He cares a lot about this. Senator Voinovich, among others. Among the issues that I think keeps us apart is the issue of preemption, how we should deal with States that have turned to—in the absence of any kind of Federal standards or approach, what States would like to do, and a handful of States have already passed, I think, legislation or are considering it. Many others are debating it.

What advice would you have? And apparently this is something you think is important, the Department, the Administration thinks is important. We have got, I think, one other Committee, the Environment Committee, on which I serve, and I understand there is

some jurisdictional wrangling that is going on between our Committee and that committee that might keep us from taking up the legislation.

And the other major issue—and correct me if I am wrong, Madam Chairman, Senator Lieberman, but I think the other major issue might be preemption. There are perhaps others. But a little bit of advice would be welcome as to your willingness—maybe just, first of all, your willingness as the Secretary to work with some of our colleagues on other committees to help remove a procedural road block to actually bring chemical security to the floor. We have talked about whether or not it would be offered as an amendment. The Republican Leader in the Senate does not want to waste a lot of time on legislation that would get bogged down in a food fight on chemical security. And we do not want to spend a whole lot of time on trying to figure out what is the right thing to do on preemption, when we are, Democrats and Republicans—it is not a partisan issue. It is just that people have different views.

One, your thoughts on how hard you are willing to push to try to get something done on chemical security, and opportunities, as we do port security legislation this week, could be offered as an amendment. I think some folks are offering rail security, transit security, which I very much support. But rather than give a good testimony, what can you do to help us actually get something done this week?

Secretary CHERTOFF. Well, I know that we have been working very closely with this Committee and other committees on both sides of the Capitol on this issue. My desire is to get a chemical security bill that gives us the authority to do what we are poised to do for that gap area that we do not have the authority. And I also do not want to let the perfect be the enemy of the good, so what I have told the lawyers who are deeply involved in working on this with people on the Hill is to focus on what are the essential issues.

What I am totally unqualified to do is to opine on the ins and outs of the legislative process and to give advice as to how to best manage through the various committees and the various vehicles.

Senator CARPER. Could I interrupt for just a second? I spent 8 years as a governor, and I was not supposed to be an expert about that stuff either, but I was. And, frankly, you have been at this job—you are good. I have a lot of respect for you. But you need to have your antenna and your focus on that as well.

When you sit there and you tell us chemical security is a major priority of this Department, if you are not prepared to weigh in here, roll up your sleeves, and try to get something done, it is not as helpful as it might otherwise be.

Secretary CHERTOFF. Well, I think we have been doing that, and I think we have been up—and I have talked to not just the Chairman——

Senator CARPER. If I can interrupt again, Senator Voinovich has just come back in. We are talking about chemical security. We are talking about jurisdictional disputes here that might preclude our getting something done. We are talking about the issues of preemption, which I know you have a lot of interest in, too. And I am try-

ing to enlist the Secretary's active participation in getting some progress here.

Secretary CHERTOFF. As I say, I spoke to the Chairman, I spoke to the Ranking Member over the last several months, I spoke to members of the House leadership, leaders in the House, all trying to forge what I thought was a workable compromise which would get us the authority to do what we need to do by regulation.

I guess my advice would be to keep it as simple as possible, that the more that is laid on something, my observation has been, the greater the likelihood it will not navigate through the very narrow channel which is available to move something like this on. And particularly because what we may get in the short term may not be the ideal solution, but it will get us a good deal of the way to an ideal solution.

My weigh-in on this would be let's take the simplest vehicle possible, the one with the highest likelihood of success in both Houses, and let's try to get that done. And if it turns out that we want to add to it later or with the experience of time it is inadequate, that is fine. But we actually can do a lot now, even with the most bare bones type of thing which is out there, and so that is for someone who is in the Peanut Gallery, so to speak, that is my coaching.

Senator CARPER. Well, you are not in the Peanut Gallery. We are in the car, and these two folks are like—one is driving, and the other is riding shotgun, and the rest of the Committee is in the back seat. You are not far away.

Secretary Chertoff. I am in the trunk? [Laughter.]

Senator CARPER. We are going to keep you out of that trunk.

Chairman COLLINS. He wants you to be the engine.

Senator CARPER. That is good.

Chairman COLLINS. Don't sound surprised.

Senator CARPER. The other thing I wanted to mention, if I can, Madam Chairman, to go back to rail security, there are a bunch of tunnels that go into New York City. Every day they carry, I am told, hundreds of thousands of people in and out of New York City. They are submerged. I don't know what body of water they go under—the Hudson River or the East River?

Secretary CHERTOFF. Hudson River.

Senator CARPER. But they carry a lot of people. I am told that if there was an explosion on any one of those commuter trains or, for that matter, Amtrak trains, it could not only hurt a lot of people on the train, but could actually puncture a tunnel, cause flooding into the tunnel, flood that tunnel. The water could back into the Penn Station and flood the other tunnels as well and create great havoc and loss of life.

When I look at threats on the rail transit side, that to me is like a preeminent threat. You have other threats that include tunnels under Washington, DC, and Baltimore. You have a lot of bridges between here and New York City and Boston that are important as well.

When you consider transit and rail security in terms of actually prioritizing what needs to be done, how do you set those priorities? What are the priorities? And how are we doing a better job today in rail and transit security than we were a couple of years ago? And how do you see us doing even better in the next year or two?

Secretary CHERTOFF. Well, actually, Senator, that is exactly what we do. We looked at exactly the issue you talked about. In fact, this past year—in the past, we had looked at the issue of rail transit and mass transit in terms of amount of trackage, and what we did is we changed that, so now we look at trackage underground as opposed to—we tier it. We have aboveground, underground, and then underground in tunnels that are underwater, of which the third is the highest priority for precisely the reason you talk about. And without saying it in an open hearing, much of our transit grant decisionmaking this last year for the first time was driven precisely by a recognition that the consequences of something occurring in a tunnel underwater are significantly greater than the same event occurring on a stretch of track aboveground. And that is exactly the disciplined approach we want to take. We have tried to inject, among other things, real science into this process now.

So I would envision that we will continue to push a significant amount of the money on a risk basis to precisely those elements of the rail infrastructure that have the greatest vulnerability.

Senator CARPER. All right. Thanks. The last thing I would say, if I may, Madam Chairman, going back to the issue of chemical security, I would urge you to be proactive today, this week, next week. Thanks very much.

Chairman COLLINS. Thank you.

Mr. Secretary, thank you so much for your testimony here today. We obviously could keep you for several more hours, but you are in luck that we have several more witnesses. So thank you very much for your excellent presentation.

Senator LAUTENBERG. Madam Chairman, will the record remain open?

Chairman COLLINS. The record will stay open for 15 days, as it always does, for the submission——

Senator LIEBERMAN. Madam Chairman, if I may end on a light note. Mr. Secretary, I think you made a generationally sensitive comment about the Peanut Gallery before. If I remember from my youth, that was a term coined during the Howdy Doody television show, and I prefer to think of you not as a member of the Peanut Gallery but as Buffalo Bob. [Laughter.]

Secretary CHERTOFF. I actually thought it was a baseball expression from when you were back in the bleachers, but——

Chairman COLLINS. I must say this is all completely lost on me.

Senator LIEBERMAN. For obvious reasons. [Laughter.]

Chairman COLLINS. Senator Pryor has just arrived, and Secretary Chertoff, I want to give him the opportunity, if he does want to ask a question.

Senator PRYOR. That is OK.

Chairman COLLINS. OK. Thank you, Mr. Secretary.

I am going to call forward both our second and third panels in the interest of time. We are very pleased to have such distinguished witnesses with us today: Sheriff Leroy Baca and Deputy Commissioner Richard Falkenrath, as well as Steven Simon and also Daniel Prieto.

Sheriff Baca is the Sheriff of Los Angeles County and commands the largest Sheriff's Department in the United States. He is also Director of Homeland Security-Mutual Aid for California Region I,

which serves 13 million people. I want to say that I had the pleasure of meeting the sheriff through Representative Jane Harman on two trips to the L.A. area, and I was so impressed with the work that he is doing to strengthen the region's defenses against terrorism.

Dr. Richard Falkenrath was named the Deputy Commissioner for Counterterrorism in the New York Police Department in July. Prior to joining the NYPD, he was a Fellow at The Brookings Institution, and from 2001 to 2004, he served on the White House staff, including serving as the First Deputy Assistant to the President for Homeland Security.

Steven Simon is Senior Fellow for Middle Eastern Studies at the Council on Foreign Relations and co-author of the book, *The Next Attack*.

Daniel Prieto is the Director and Senior Fellow of Homeland Security Center at the Reform Institute. Previously, he was the Research Director of the Homeland Security Partnership and Initiative, as well as a Fellow at the John F. Kennedy School of Government at Harvard.

We welcome all four of our distinguished experts here today. I want to apologize to you for your having to wait so long. We had a greater attendance than we expected today in view of the importance of the issues before us.

Sheriff Baca, we are going to begin with you.

TESTIMONY OF LEROY D. BACA,[1] SHERIFF, LOS ANGELES COUNTY, CALIFORNIA

Mr. BACA. Thank you, Madam Chairman, and thank you, Ranking Member Senator Lieberman, and Members of the Committee, which I know have other things to do, and I realize that time is short. I have seven points and six categorical recommendations to make, and I would like to say that Los Angeles County is one of America's engines for imagination and innovation when it comes to public safety in view of this recent responsibility of homeland security and terrorism.

The first point on the categorical side here is that California is a formal mutual aid State. It has been that way since 1950. We have a very defined system in law where local government is enabled by State support, through counties as well, and that the mutual aid system that we use has been well in place and time-tested. Whether it comes to earthquakes, fires, any incident of disturbances or attacks, emergency activities included, we know what to do.

Second, California sheriffs are mutual aid coordinators, which means it is an integral part of the governmental process and governance for mutual aid and first responders. In the case of California, and Los Angeles County in particular, each regional area—and I happen to be in command of Area I, which includes two counties, Orange County and Los Angeles County—we serve 10 million people and, therefore, organize over 50 police departments and over 40 fire departments in whatever we do in a mutual aid context. And therein the law enforcement mutual aid coordinator, there is

[1] The prepared statement of Mr. Baca appears in the Appendix on page 69.

a need for us to operate in an area that includes multi-level governance. And that is the operating interoperable side of how you manage something in that you have many governments working together to work at solving a problem.

The third point I will make is that we had developed a Terrorist Early Warning Group System prior to September 11. Although more than 5 years have elapsed since the tragedy of September 11, we continue to institutionalize the lessons learned of that day. We have Federal, State, and local partners, and we aggressively pursue ways to integrate our disparate agencies into a seamless network of information-sharing cooperatives. To understand where the Los Angeles County Sheriff's Department is headed, there must be an understanding of where we began.

We formed in 1996 the Terrorism Early Warning (TEW) Group System, which analyzes trends and potentials for terror attacks within Los Angeles County. The TEW now employs subject matter experts from law enforcement, the fire service, public health, academia, and the military, all working together to ensure the safety of Los Angeles County residents. Representatives from the FBI and the Department of Homeland Security also work within the TEW to produce high-quality, analytical products that are provided to decisionmakers covering a variety of subjects related to terrorism.

The fourth point is our Joint Regional Intelligence Center of Southern California that was mentioned earlier. Recognizing the value of cooperation between Federal, State, and local agencies, leaders from the FBI, the U.S. Attorney General's Office, the State Office of Homeland Security, Los Angeles Police Department, and the Los Angeles County Sheriff's Department decided more than 2 years ago to join together and create a model for intelligence fusion centers. The vision became reality in July 2006 with the grand opening of the Los Angeles Joint Regional Intelligence Center and Mr. Chertoff was there.

Using analytical processes developed by the TEW, analysts from a variety of agencies and disciplines create an expansive view of trends and potentials that could indicate a potential terrorist attack. The U.S. Department of Homeland Security was also present at this center, and the components of that Department, such as Customs and Border Protection, Immigration and Customs Enforcement, Transportation Security Agency, and the Coast Guard, are contributing personnel to this organization. These agencies possess critical information that must be synthesized with local products to make the forecast of potential threats clear. I strongly encourage the participation of any public agency involved in issues of homeland security with its local TEW fusion center to do exactly what we are doing in Los Angeles.

Fifth, we have terrorism liaison officers. This is necessary to keep the coordination of communication going on an ongoing basis.

Sixth, there is a formal private sector outreach and partnership. It is called the Homeland Security Advisory Council. It is chaired by Marc Nathanson, founder of Falcon Cable Corporation. We have every possible source of the business community involved in this, and we work this Committee very hard in a partnership with the National Security—it is called the Business Executives for National Security (BENS), based here in Washington, and therein inte-

grating the private sector into our intelligence process. This is a very big part of what we do through infrastructure liaison officers. The infrastructure liaison program further expands the network of trusted agents to include people dedicated to the critical infrastructure protection. This addition to our intelligence process creates a comprehensive network that provides a better opportunity for the prevention, disruption, or mitigation of a terrorist attack.

I wanted to commend Senator Voinovich for his thoughts concerning the Muslim American society. We have a formal Muslim American outreach and partnership program. Another key component to our strategy is our connection to the Muslim community through the creation of the Muslim American Homeland Security Congress. Consisting of respected leaders from Muslim organizations within Southern California, their mission is to foster communication, education, and mutual respect between law enforcement and the Muslim community. Programs such as our Homeland Security Advisory Council and our Muslim American Homeland Security Congress are reflective of our belief that homeland security is not an issue that can be resolved through traditional police practices only.

This program will be moving itself to Chicago, and I will be traveling with its leaders to Detroit, where our largest Muslim American ghetto exists, so that we can further empower Muslims to speak up in the securing of our homeland mission here in the United States, as well as in nations abroad.

For the next 5 years—and you have heard this, and I will just be very brief so the others can speak. What do we do in the next 5 years? Well, there are seven things I would like to say.

First is communications, and you have talked about interoperability so I do not need to continue to focus on that. But it is a gap that needs to be closed. Second, intelligence must be shared vertically and horizontally across jurisdictions for analysis, investigative, and operational purposes. Those are three key components to intelligence: Analysis, investigative, and operational purposes.

The second point is technology as a general subject. Surveillance technology needs additional development and standards. There are a lot of things going on out there in the world of surveillance, but we do need to have better standards on a national scale.

The next point under technology is detection technology, on which we heard a significant amount of comment here by the Senators and Secretary Chertoff. Detection technology for chemical, biological, and radiological applications needs additional development as well. I think that is clear.

The next point is national technology resources need further logistical development for regional and national application. In other words, I am talking about shared classified technology. For example, the Department of Defense and the National Intelligence Community have equipment that local police do not have, and we would like to see further access to that opportunity to use the equipment.

Finally under the point of technology, research and development of new technology should be jointly managed to avoid wasteful duplication. This should be managed by a national board of volunteer Federal, State, and local intelligence and first responder experts.

My third point on what can we do in the next 5 years is to develop a joint forces training center, a system throughout the United States. In other words, develop three or more training centers on terrorism for Federal, State, and local first responders and intelligence first responders of terrorist acts. Currently, the California National Guard and the California Mutual Aid Region I, which is Los Angeles and Orange Counties, are developing this proposal, and we think it can be a model for the rest of the Nation.

My fourth point is international cooperation, training, best practices, and personnel exchanges should be expanded. I have traveled to Jordan after the Amman bombings. I have traveled to London after the bombings there with the train stations. I have traveled to Israel. I have been to Turkey after the bombings that have occurred there. And this is a very critical part of how we all learn about what is going on in different parts of the world. Current plans are underway to have training in Paris, France, at the Interpol Headquarters led by cities and countries that have experienced a terrorist attack. I think we should take every major target city in America and have those police chiefs and firefighter leaders, along with their mutual aid coordinators, go to this conference so that they can hear directly from these countries as to how they managed the particular terrorist attacks they have endured.

The fifth point is to continue to fund the National Terrorism Early Warning Resource Center that partners with local and State law enforcement. There are currently 26 local terrorist early warning systems in our Nation today. The long-range vision and effort is to link more than 50 terrorist early warning systems across the country with other local and State fusion centers, such as the Joint Regional Intelligence Center in Los Angeles.

Sixth, the Department of Homeland Security's major policies—I wish Mr. Chertoff was here, but I have told him this before—should be developed in partnership with selected experienced local, State, and Federal law enforcement leaders in deciding financial, operational, and training policies. The UASI grant program is one example where we can improve significantly in what we are doing.

Thank you for listening to my comments. They have been very brief in their content. I am talking about unified government, unified first responder planning, and I am talking about unified leadership, which is what American society wants today on this subject of terrorism.

Thank you very much.

Chairman COLLINS. Thank you, Sheriff.

Mr. BACA. And I have copies of my testimony here.

Chairman COLLINS. Thank you. Your full statement will be put in the record.

Dr. Falkenrath.

TESTIMONY OF RICHARD A. FALKENRATH, PH.D.,[1] DEPUTY COMMISSIONER FOR COUNTERTERRORISM, NEW YORK CITY POLICE DEPARTMENT

Mr. FALKENRATH. Thank you, Madam Chairman. It is always an honor to be at this Committee, which did so much important legislation in the last 5 years for the country.

I want to start by saying a few words about my new job in New York City in the New York City Police Department. I think as everyone knows, we are the biggest and most densely populated city in the country. We have a population of 8 million people; 40 percent are foreign born. The most diverse, ethnically diverse county in America is Queens County. The gross metropolitan product of New York City and its surrounding areas is $900 billion. That is larger than all but about a dozen countries. The New York City Police Department has 52,000 personnel, a budget of just under $4 billion. That puts it on the order, in terms of size, with most armies in the world.

We have created a Counterterrorism Bureau and dramatically expanded the Intelligence Division since September 11. The Counterterrorism Bureau I have the privilege of now heading. The Intelligence Division is headed for the last 4½ years by a former Deputy Director of Operations of the CIA, backed up by a former Deputy Director of Intelligence for the CIA who runs our intelligence shop. All together, we have about 1,000 officers dedicated to counterterrorism and intelligence missions and a total budget of on the order of $200 million per year.

We have about 110 to 120 NYPD detectives assigned to the Joint Terrorism Task Force at the FBI. They all report to me. In addition, we do a very wide range of training and other programmatic activities, both for our own people, our partners inside the city, other State and local agencies, Federal Government agencies, and international agencies from time to time.

We have a cadre of civilian analysts whom we have hired since September 11 who are as good as any I saw when I served in the White House. They are headed by a Rhodes scholar and former Supreme Court clerk. We have an outreach program to the private sector.

The list goes on, and I catalogue this in my prepared statement, which I ask be submitted to the record.

Chairman COLLINS. Without objection.

Mr. FALKENRATH. The extent of the special events we need to handle in New York City is shown this week. Yesterday we had the commemoration of September 11. The President of the United States was there. Next week, he is coming back, along with 159 other heads of State. It is the largest, regularly scheduled meeting of heads of state in the world, the UN General Assembly. We do it every year, have been doing it for 50 years, and know how to do it pretty well.

This is who we are. New York City had to respond after September 11 in this way and did. The same could also be said in different ways of the other New York City agencies—the Fire Depart-

[1] The prepared statement of Mr. Falkenrath appears in the Appendix on page 74.

ment, OEM. They have also stepped up. It just so happens that I am the one testifying today.

A word on the threat. In my testimony, I list 18 recent encounters that New York City has had with international terrorism in the past 15 years. They have repeatedly targeted New York City. That is why we take it so seriously. The most recent threat and plot came to light just a couple months ago when a leak revealed an extremely sensitive intelligence investigation into an ongoing threat against one of our tunnels and, in fact, against a critical piece of infrastructure.

We view the threat to the city as a global phenomenon, and hence, we take a global view, which can manifest in our city at any moment in almost any way. We do not confine our work and our analysis to the five boroughs for which we have direct responsibility.

Globally, clearly on the good side, we have seen a reduction in legacy al-Qaeda which attacked us on September 11 to a fraction of what it was before. This is good. We have also seen an improvement in our border security, which has made it somewhat more difficult for international terrorists to get into the United States to conduct attacks. We do not take any comfort from that because the baseline vulnerability was so high, but there has been some progress.

Aside from those two items, though, I would say most of the other indicators are bad. We have seen the proliferation of extremist Muslim ideology, Muslim militancy, and Salafism, which we think is a precursor to terrorism. That proliferation, that spread of that ideology has been very well documented abroad. A lot of people write about that. They talk about it on television. We have observed it, and we have hard evidence of it in New York City as well. It has us very worried, and I would add, in many surrounding areas, not just in the five boroughs.

The homegrown threat you referenced, Madam Chairman, in your question to Secretary Chertoff we are very worried about. These are the most common forms of attacks since, and there are important implications for how we conduct counterterrorism operations if we take the homegrown threat seriously, which I will reference. We have seen increasing use of the Internet, of course. The threat is very serious. I wake up every morning thinking today might well be the day that we get another attack in our city.

Now, recommendations. At your request, we will give a few. They will not be confined just to issues of immediate interest and concern to NYPD, but I will base them on that.

First, with respect to Federal counterterrorism, we note that the vast preponderance of Federal effort—money spent, hours spent by Federal personnel—is international in character. It focuses on collecting and countering international threats. The domestic counterterrorism effort that we have is most powerfully predicated on this international effort. Most of the high-profile investigations that we have in the United States are begun because of a lead that was generated abroad, and those are very important. And the FBI has made a huge amount of progress conducting those sorts of investigations. We work with them very closely, and we now, I am

happy to say, have an excellent partnership with the FBI for those sorts of investigations.

We have a problem, however, when you deal with a homegrown threat, which has no international connectivity or limited international connectivity for which your massive national technical collection abroad is unlikely to give you a predicate to begin an investigation. Then the question is: How do we find out about it in the first place? And there the answer is far more likely to be found in the structure of law enforcement-driven, local, highly tactical intelligence programs of the sort we conduct.

Second, on information sharing. The Federal Government has a plan or a vision for how information sharing is supposed to work between Washington and State and local agencies, such as my own. We are not sure what it is. There is a lot of different information sharing going on. Occasionally it is useful. Mostly it is not. The one that is consistently useful is the sharing of classified information done in the context of the JTTF. That works reasonably well for what it is. We have several hundred personnel with top secret security clearances, so we are able to handle that. Not all agencies are.

The important thing I would say here is the Federal Government cannot try to control this. If they try to tightly control it, if they have one single pipeline to the State and local issues, it is sure to fail. And so I hope they do not go down that road.

On the watchlist, a couple questions on this one. I believe we have an integrated terrorist watchlist in this country. The question is how well do we screen against it and when do we screen against it. When we book somebody at NYPD, they are always checked against the terrorist watchlist because we do a national criminal records check, and that is linked up with the TSC watchlist and that is good. There are many other areas, though, where we could be screening where we are not. When you get on an airplane to fly from New York to Washington, DC, you are not screened electronically against a watchlist. Secretary Chertoff and others here in Washington need to be working on that.

Critical infrastructure protection. I have a lot to say on it. I spend a lot of my time on this now that I am in New York. For us, it is very tactical. It is about super-high-value targets, and we catalogue them. We have studied them. I have a list of what we deem to be the 30 or so most dangerous targets in New York City. We guard it carefully, and we work on them to try to reduce it.

What we do will depend on the case. In some cases, we might close a street. We might put up a vehicle screening center. We might put bollards in. We might work with the real estate developer or the owner to enforce better standards in their design for blast resistance.

On this I would say we are pretty much on our own. We do not get a lot of help from Washington. If Washington wanted to do something, it could set a standard for building codes that would include blast resistance and performance standards. There is no such thing. And it would get a policy on terrorism risk insurance. Right now commercial policies do not insure against terrorism risk and, hence, the private sector has no financial incentive to take really prudent measures against it. They are assuming that the Congress

will insure them, that if there is an attack, they will just buy them out. So there is no terrorism risk insurance anymore. And if you wanted to do something, that would make a difference.

The five last items, and then I will stop. Chemical security, you know my views on this. I hope something gets done in this Congress and to the President's desk. That would be great. As a legislative handicapper, I would have to say the odds are long. It is late in the season to be doing this. But if it happens, great; otherwise, it is to the 110th Congress. We will be disappointed, but we have been disappointed before on that.

I would, however, want to state something on ANFO, ammonium nitrate and fuel oil. This is the most common explosive. It was the one that was used in Oklahoma City to take down the Alfred P. Murrah Federal building. It was procured legally and easily by those two bombers, and since then we have done nothing—nothing—federally to improve the security of ammonium nitrate fertilizer.

When you combine it with fuel oil and it is sold precombined, it is governed by Title 18 criminal codes. Separately—they can be easily combined. Separately, they are not governed by anything. We conducted a test, a special project to go to upstate New York and other areas to buy fuel oil and ammonium nitrate fertilizer to build a bomb. We did it with no difficulty whatsoever. We got companies, in fact, to deliver supplies and materials to Brooklyn, tripping no wires. And we built it in a warehouse in the Bronx. All right. Case in point. So do not exclude ammonium nitrate from your chemical security legislation.

On mass transit, in a very real way mass transit security is New York's security. A couple statistics. In 10 weeks, more people ride the New York City subway than ride all airplanes in the entire country all year. One-third of all mass transit rides in the country are on the New York City mass transit system. If you look just at subways, 65 percent of all subway rides in this country are in New York City. The terrorists are attacking the subway system worldwide. We think that means they are likely to come at ours, which is hugely vulnerable. The Federal Government has spent $9 for every air passenger in the country and 0.6 cents on every mass transit passenger in the country. There is something wrong with this, so if government were to be able to do a little bit there, it would help.

We have 2,700 mass transit cops who never come aboveground during their duty. They stay underground, and that is their whole job, and they do it on their own with no Federal assistance to secure that.

Ports. I think on the port security, I think this town is focused on the wrong part of port security. It has been on the container security problem. The real problem, in my judgment, is what al-Qaeda has done before when they attacked the Cole, which is a small, explosive-laden boat brought up against a passenger ferry or a critical infrastructure facility, and it is security on the water. And there, again, we are doing it more or less on our own. The Coast Guard helps out a little bit. They are great partners, but they are really not in New York harbor. It is mostly done by New Jersey State Police and NYPD Harbor Patrol.

The last thing I will say on grants. We have big problems with how the Federal Government has done grants. That is well known. I would say six things.

First, the overall level of grants from the Federal Government to the State and local agencies right now nationwide is indefensibly low. The President proposed in February 2002 $3.5 billion. The level now, depending on what comes out of the conference report, is going to be about $1.6, $1.7 billion for the whole country for the whole year in 2007. That is nearly a $2 billion reduction. That is too low, particularly when we are spending $10 billion per month in Iraq. It just makes no sense.

Second, we believe 100 percent of the Federal money should be risk-based, just like the 9/11 Commission, which in its review of the implementation of its recommendations gave the Congress an F on that matter. That is their opinion.

Third, of the State grants, we think those need to be distributed by the governors on the basis of risk, not spread around to all the outlying areas as they wish. DHS, when it distributes money based on risk, needs to get a comprehensive and coherent way of doing it. We don't think they have one now.

Finally, I would say DHS needs to permit the charging of operational expenses that are dedicated to counterterrorism and intelligence activities, separate and distinct units, to the grants. They do not currently allow that. If you want to buy equipment, that is great. If you want to conduct an exercise, that is great. If you want to do a study with Booz Allen or SAIC, that is great. But if you want to pay for an intelligence operative who is working in a high-threat area, in a very dangerous area with a lot of Muslim extremism, no, you cannot charge that.

The last thing, I sincerely hope that the Congress does not condition the disbursement of Federal grants on city confidentiality policies with respect to immigration. This is a very divisive issue in this country, immigration, and there is an idea in the House mark-up that you should not give any money to any city that prohibits its employees from talking to ICE about a person's immigration status. New York City happens to prohibit that in some cases. If the House bill became law, by definition we would get no money, and this would be a bad idea. It does not make any sense to hold the city hostage to the country's ongoing dispute about immigration. Thank you for your time.

Chairman COLLINS. Thank you. Mr. Simon.

TESTIMONY OF STEVEN N. SIMON,[1] HASIB J. SABBAGH SENIOR FELLOW FOR MIDDLE EASTERN STUDIES, COUNCIL ON FOREIGN RELATIONS

Mr. SIMON. Thank you, Madam Chairman. I am grateful for the opportunity to address the Committee on this vital topic.

My understanding of the Committee's objectives in holding this hearing is that witnesses should focus on the future and address themselves to issues that might help both Congress and the Executive Branch set homeland security priorities. The Committee, it seems to me, is doing the right thing.

[1] The prepared statement of Mr. Simon appears in the Appendix on page 106.

I have some very personal reflections on this issue that are fairly broad-brush that I would like to share with you. I am going to concentrate on three issues in particular.

First, the importance of cities as terrorist havens and terrorist targets. There has been a lot of talk about that in these statements, and the talk is well placed. Second, I am going to address myself to the continuing significance to many jihadists of weapons of mass destruction. And, third, to the need to preserve the good will and sense of belonging of America's Muslim communities as a matter of national security beyond the intrinsic virtues of a cohesive, considerate society in which citizens of all creeds can feel at home.

On urban warfare, the crucial point is that the jihad that has evolved since September 11, 2001, has become a war of cities. The transition from caves to condos, as one observer described the evolution, has been impressive. The relatively remote, rural bases that incubated the jihad had strong advantages, especially given the importance of social networks to the jihad, but municipalities have their own attractions, as other witnesses have indicated. They offer anonymity, but also community, both of which can confer a kind of cover.

Urban neighborhoods, with their numberless apartments, coffee houses, mosques, and Islamic centers, provide the setting for recruitment, clandestine meetings, preparation of weapons, and other activities that form the terrorist enterprise. They are not subject to Hellfire missile strikes or submarine-launched cruise missiles or things like that. Those tools will not work against this kind of presence. Think of Mohamed Atta's Hamburg or the Leeds of Muhammad Siddique Khan, who was the orchestrator of the July 7, 2005 bombings.

Qualities that favor the jihadists' defensive requirements do not tell the whole story. However, the other side is that cities are where their targets—both symbolic and of flesh-and-blood—are to be found in abundance and proximity.

New York, as my colleague here has indicated, has shown itself to be a crucial target for jihadists. This great city was construed by al-Qaeda to be the beating heart of America's economy, which bin Laden believed he could cripple; the symbol of American arrogance as embodied by the "looming towers" of the World Trade Center; and the seat, of course, of Jewish power, which jihadists believe accounts for the global subordination of Muslim interests to America and Israel. It is also a teeming city, whose large and densely packed population promised the most efficient path to a successful mass attack that, from a jihadist standpoint, might even begin to settle the score with the United States. There is no reason to think that this conviction has weakened. Furthermore, New York City proffers the same advantages to the attacker as do all large cities.

The array of targeting opportunities, I might add, in New York, as well as in other large cities in the United States, particularly Los Angeles, as Sheriff Baca has indicated, is quite wide. We can be perversely certain that an attack, when it comes, will be the one we least expected, but one can make some preliminary judgments. Mass transportation, as has been indicated, symbols of authority,

financial districts, and, we should bear in mind, schools as well, given the importance in jihadi propaganda to the depredations that the United States has carried out against Muslim children, either directly or through Israeli allies.

Improvised explosive devices like car bombs—the icon of urban violence in Iraq and elsewhere—we can expect, as well as Palestinian-style backpack bombs.

Now, the implication of this analysis, I hasten to add, is that community policing and extensive video surveillance will need to be stepped up. In this kind of urban warfare, intelligence is acquired best by those who are most familiar with the terrain: Police officers walking their beat. On the front line, they get to know their neighborhoods, the residents and the shopkeepers, form and cultivate relationships with local citizens, and develop a sense of the natural order of things and, therefore, of signs that something is out of the ordinary or warrants investigation. The pivotal role of local law enforcement is reinforced by the incapacity at this time of Federal authorities to gather information skillfully, discreetly, effectively, and without alienating potential sources of intelligence. The FBI, in particular, presently lacks the numbers, skills, knowledge base, and orientation to contribute.

This does not mean, as my colleagues here have said, that local law enforcement can or should operate in a vacuum, especially in light of connections that have been disclosed between the self-starter groups in the United Kingdom and al-Qaeda figures in Pakistan. On the contrary, local police need an umbilical connection to national intelligence agencies in order to connect the dots they are collecting on the ground. It is worth noting, by the way, that the success of the U.K. counterterrorism effort in Northern Ireland was largely due to the tight linkages between the local police, national police, and Britain's domestic intelligence agency that were forged early in the conflict.

Information sharing, which all parties now claim to be essential, has not advanced significantly, and to illustrate this point, I will just note that, at most, less than 1 percent of the detectives or police officers in the United States have security clearances that enable them to receive relevant and operational kinds of information from Federal agencies. This is a circle that clearly needs to widen.

The other issue we need to focus on is where the police officers who will be collecting these dots I referred to are going to come from. In the upcoming Federal budget cycle, the COPS program is again under pressure to be cut. This program has put more than 100,000 policemen on the street. It is an invaluable program for American counterterrorist interests at home.

Very briefly, I wanted to highlight the continuing importance to jihadists of weapons of mass destruction. On the basis of 10 years of dealing with their documents and intelligence about them and so forth, I can guarantee to you that they are very interested still in acquiring, deploying, and using weapons of mass destruction. This puts a premium on consequence management. That is the only aspect of this problem I will highlight. It will be essential in the wake of an attack, and it will be very difficult to prevent a successful attack—that is to say, it will be very difficult to prevent a well-planned attack. We must be able to respond at the Federal, State,

and local levels in lockstep and with the appearance and reality of deep, deep competence. This will be essential to preserving the fabric of our society in the wake of an attack and deterring further attacks.

In operational terms, what I recommend is that there be a single Federal enforceable standard for State and local capacities for consequence management. Right now in the United States, we are all over the place. The Federal Government needs to establish a standard, establish milestones and benchmarks. This is not just a matter of appropriating funds, but ensuring that cities meet a given standard.

Finally, the September 11 disaster showed that skilled and self-possessed and highly determined attackers could do tremendous damage to the homeland without an infrastructure. But that is not the only way things work. It is not the adversary's sole option. Other approaches do require infrastructure, in the shape of cells that may or may not be linked to outside networks.

We have a potential problem in the United States with our Muslim citizens. According to recent research, they are increasingly choosing not to assimilate into American society. They have been under huge pressure since September 11. This is having its effect. They are finding solace instead in their religious identity. Muslim student associations on college campuses are growing rapidly as havens for Muslims who prefer not to socialize with non-Muslims, and Muslims are building Islamic schools as alternatives to the public school system, which is perceived as inhospitable. They are trying to thwart media bias by developing their own radio stations and so forth.

These are telltale signs of a growing problem, and the evolving attitudes of non-Muslim Americans toward their Muslim compatriots are also likely to spur alienation. According to a 2006 Gallup poll, a third of Americans admire "nothing" about the Muslim world, and nearly half of all Americans believe the U.S. Government should restrict the civil liberties of Muslim Americans. This is increasing the pressure on our Muslim citizens.

Now, of course, they have shown no sign of violent protest. We really should be sure to keep it that way.

Now, I have put this issue before the Committee for lack of a better place. The challenge outlined here requires leadership and a program, yet given the way our government is structured, there is no obvious lead agency or Special Assistant to the President on the National Security Council or Homeland Security Council to formulate a program to provide such leadership.

We are not the first to face this conundrum. Several years ago, in the wake of a Whitehall study showing upwards of 10,000 al-Qaeda supporters in Great Britain, Her Majesty's government tasked the Security Service—MI5—both to dismantle jihadist networks and devise a plan to win the hearts and minds of Britain's Muslim minority. Ultimately, the Security Service balked at the difficult job for which they had no experience or clear jurisdiction. We need to do better. Fortunately, unlike our sister democracies across the Atlantic, we have time, and I urge you not to squander it.

Thank you.

Chairman COLLINS. Thank you. Mr. Prieto.

TESTIMONY OF DANIEL B. PRIETO,[1] SENIOR FELLOW AND DIRECTOR, HOMELAND SECURITY CENTER, REFORM INSTITUTE

Mr. PRIETO. Thank you very much, Chairman Collins and distinguished Members of the Committee on Homeland Security and Governmental Affairs.

My name is Daniel Prieto. I am Director of the Homeland Security Center at the Reform Institute. I want to thank you for inviting me to testify before you today on the topic of "Homeland Security: The Next 5 Years."

At the 5-year anniversary of September 11, the question is unavoidable: Is it safe? Dustin Hoffman's answer to that question in the 1976 movie "The Marathon Man" was alternately, "Yes," "No," and "It depends." The same is true when it comes to homeland security. For every area of progress, significant gaps and vulnerabilities remain.

In many ways we are safer. Members of the Committee and the previous speakers have outlined many areas where we have made progress. But in many ways we are not safer. Five years from now, there are five areas where we need to make significant progress.

One, we have not fully engaged our citizens and captains of industry to protect America.

Two, we lack a national consensus on priorities, and our supposed strategies are not strategic enough. As a result, it seems that we are perennially reacting to the latest threat.

Three, DHS struggles to meet the expectations that accompanied its creation. Management is key.

Four, as the Nation that invented Silicon Valley, the Internet, and companies like Microsoft and Google, we are the technology envy of the world, but the government cannot seem to get it right when it comes to important homeland security technology projects.

And, five, information sharing is very much a work in progress, and, in particular, on controversial data-mining programs, we are forcing the trade-off of liberty for security in an unnecessarily zero-sum game.

To start out on the first point, we need to engage society better, both citizens and the private sector. The inaugural National Strategy for Homeland Security argued that "the Administration's approach to homeland security is based on the principles of shared responsibility and partnership with the Congress, State and local governments, the private sector, and the American people." While that sentiment was and is correct, we have failed to execute on it. We have done too little to engage and educate the public. Too many policymakers tend to view the general public not as a source of strength, but as either victims or prone to panic. Too many officials fear that too much information provided to the public will either frighten them or aid our enemies.

This discussion should end. The more informed and self-reliant we are when the next attack or disaster strikes, the better off we

[1] The prepared statement of Mr. Prieto appears in the Appendix on page 113.

will be. The United States will win the war on terrorism not by force of arms alone, but by the resolve and resiliency of its citizens.

Brian Jenkins of the RAND Corporation puts it best in his new book, *Unconquerable Nation*: "We need to aggressively educate the public through all media, in the classrooms, at town halls, in civic meetings, through professional organizations, and in volunteer groups. . . . The basic course should include how to deal with the spectrum of threats we face, from 'dirty bombs' to natural epidemics, with the emphasis on sound, easy-to-understand science aimed at dispelling mythology and inoculating the community against alarming rumors and panic."

In addition to educating the public, we need to get to a point where public-private partnership for homeland security is more reality than rhetoric. Five years after September 11, the capabilities, assets, and good will of the private sector to bolster our homeland security remain largely untapped.

Second, homeland security needs to move from tactics toward doctrine, especially when it comes to preparedness and on critical infrastructure. While many security strategy documents have been produced since 2001, most of them are largely documents about tactics, methods, and processes. As such, they fail to articulate the strategy and doctrine which can guide implementation and provide goals with which programs can be measured. This is particularly true, as I mentioned before, in the areas of preparedness and critical infrastructure.

On preparedness, we need to create a homeland security doctrine that takes a lesson from U.S. military doctrine. If our armed forces through much of the last 50 years had to be ready to fight two simultaneous wars in different theaters, then DHS, the National Guard, NORTHCOM, and State, local, and other Federal authorities should be prepared to confront two to three simultaneous large-scale homeland security events of the kind envisioned by the 15 DHS National Planning Scenarios.

In support of such doctrine, I see the creation of National Guard Special Forces providing specialized and regionally based training against the 15 DHS National Planning Scenarios for the National Guard. Additionally, it would make sense for NORTHCOM to have their own dedicated resources. They are currently only allocated 1,000 permanent personnel and $70 million on a total DOD budget of $400 billion and 1.4 million active-duty personnel.

On critical infrastructure, we need a strategy that finally makes tough choices about priorities. We have fallen into a certain political correctness about critical infrastructure as if all sectors—computers versus cows versus chemicals—pose equal risks. They do not. Some sectors are more important than others. In my view, this Committee is doing a very good job looking at those priorities because, in my view, the priorities are chemical facilities, transportation with an increased focus on mass transit and hazmat transport in addition to airplanes, and energy, including oil, gas, and the electric grid.

As a number of the other speakers have mentioned as well, it is obviously extremely important to focus on regional concentrations of critical infrastructure as well.

Bills in Congress are rightly seeking to give DHS authority over chemical security. At the same time, authorities should not stop there. Congress needs to give DHS clear authority over security activities at any infrastructure sites that threaten large-scale casualties or are critical to the functioning of the U.S. economy regardless of sector. For example, DHS should have authority to regulate critical energy infrastructure sites in order to mitigate known vulnerabilities in the electric grid.

DHS also needs to display better leadership on critical infrastructure. First, DHS assumed that the market would provide sufficient incentives for companies to adequately protect critical infrastructure. That has not happened. Now DHS has sharply curtailed protective efforts and is now acting largely as a coordinator for the efforts of other agencies. This is a mistake.

Third, security investments can help the overall health of America's decaying infrastructure. The American Society of Civil Engineers recently graded American infrastructure with the grade of D. We need to do better. Security investments can make infrastructure healthier, and we need to use all of the policy tools at our disposal. I have argued repeatedly for the use of greater tax incentives to increase investment in critical infrastructure where the private sector is not doing enough.

Third, we need DHS to be a respected and successful organization, and to do that, we need to dramatically strengthen DHS management.

The birth of DHS has not been easy. For its successes, it has suffered significant failures and missteps, which in my view have seriously damaged its credibility. Hurricane Katrina was its lowest moment, but it has been beset by a number of public missteps on a host of other topics. Due to ineffectiveness or immaturity, DHS has increasingly diminished, spun off, or shed responsibilities in such areas as intelligence and information fusion, critical infrastructure protection, and post-disaster housing and health. In the most recent Federal personnel survey, DHS employees ranked their organization at or near the bottom of nearly every measure of effectiveness. Other Departments—Justice, State, the Department of Defense—too often do not view DHS as a peer organization.

DHS is falling behind, and the window of opportunity to get things right may be closing. DHS risks becoming what I call "the DMV of the Federal Government"—widely viewed as inefficient and ineffective. If DHS fails to create synergies among the many entities it inherited and to mature into a more effective organization, we will be worse off as a country.

I present these facts about DHS not as an indictment. Many of the problems were to be expected in a merger integration exercise as large and complex as this. My point in raising them is to urge this Committee to do all it can to shepherd the maturation of DHS. It may be necessary to read between the lines when senior DHS officials state that they have all the resources and capabilities they need—rosy scenarios which may be born of political expediency or pride. To the extent that DHS's shortcomings stem from underresourced or structurally weak management, it is essential to not just punish or withhold money, but to address the root of the prob-

lem by helping strengthen management capability and accountability for the long term.

To improve DHS management, key CxO level positions must be given greater power and more resources. The Chief Financial Officer, the Chief Information Officer, and the Chief Procurement Officer continue to lack effective department-wide purview and authority. Some changes implemented by Secretary Chertoff have helped, in particular, the creation of a Policy Office and an Office of Strategic Plans, as well as increasing the power of the Deputy Secretary. But an organizational chart that has 22 separate divisions reporting directly to the Deputy Secretary while failing to fully leverage the CxO positions does not make sense. Management control and integration of DHS, in my view, remain far too weak.

Fourth, get technology right. America, as I said, is the envy of the world when it comes to technology, but too many homeland security projects since September 11 have stumbled, from the FBI's virtual case file management to DHS's Homeland Security Information Network to border security systems.

To keep the country safe, we need to make serious and sustained efforts to improve how the government deals with technology.

Fifth, and then I will close, we need to develop rules for the use of consumer and company data for counterterrorism. In May 2006, it was revealed that the NSA was augmenting domestic surveillance with large-scale data analysis of consumer telephone toll records. That revelation was only the latest instance of government efforts to use data-mining and other data analysis techniques in the war on terror. There is an ongoing controversy over the government's use of private sector and consumer data for counterterrorism purposes. Many of these programs have raised little controversy. Other ones—DOD's TIA and TSA's Secure Flight—have raised concerns and public outcry and were shut down by Congress.

The growth in data analysis efforts marks the recognition of a simple truth: Our spies are not well suited to address the jihadist terrorist threat. At the same time, government programs that analyze commercial data are imperfect and risk wrongful entrapment of innocent citizens along with legitimate terrorists. That risk is magnified by the fact that the laws governing these programs are unclear.

We need to move beyond an environment where it seems different Executive Branch agencies are simply experimenting with large-scale data analysis techniques to see what works and what they can get away with. In the next 5 years, we need to move past experimentation and develop comprehensive legislation, guidelines, and rules to govern the growing use of consumer and company data in the fight against terrorism.

Within the next 5 years, Balkanized rules for the government's use of company and consumer data need to be addressed. Any attempt to harmonize those rules should focus on the full life cycle of data: Procurement, receipt, storage, use, ability to combine with other data, sharing within the government and outside of the government, encryption, anonymization, dispute, and redress.

Clear and consistent rules to govern this activity are needed so that Americans do not feel that the only relationship between civil liberties and security is a zero-sum game.

In conclusion, Bill Gates, the founder of Microsoft, has said that we always overestimate the change that will occur in 5 years and underestimate the change that will occur in 10 years. While we have made progress on homeland security in the first 5 years, many of us are frustrated by the pace of change. In the next 5 years, we have the opportunity and the duty to make America safer and more secure. Five years from now, I hope that we have exceeded our own lofty expectations.

Chairman COLLINS. Thank you.

I want to thank all of you for excellent testimony. Unfortunately, we have a vote underway that started at 12:10, so I am just going to ask one question and then submit our additional questions to the record. But our having to abbreviate the hearing in no way diminishes our gratitude to each of you for coming here today and sharing your expertise.

Sheriff Baca, my question is for you. I mentioned in my opening statement my concern about homegrown terrorists. If we increase border security but do not deal with the increasing efforts to radicalize Muslim citizens of our country, we are going to face a very serious threat.

You have mentioned an initiative that you have undertaken which seems to me to put you far ahead of the Federal Government in coming up with a strategy to engage leaders of the Muslim community, and I commend you for that. And I am very pleased to learn that you are sharing your efforts with other cities, such as Detroit. I think that is terrific.

One area of particular concern to me is the conversion and then in some cases radicalization of prison inmates, and we are holding a hearing on that issue next week. Could you share with us any thoughts you have on strategies to be used to try to prevent the radicalization of prison inmates? And do you have anything underway in that regard specifically focusing on prisons?

Mr. BACA. Currently the California Department of Corrections is aware of an incident that occurred in the city of Torrance, which is in Los Angeles County, where inmates from the State prison system became radicalized. One, upon release, expanded that radicalization to some local community people who were not from Muslim nations, but one in particular, however, was a Pakistani national who came here and became an American.

At that point, they engaged in bank robberies and were looking to fund themselves to attempt some attacks on targets that they had identified within the county. Fortunately, we intercepted them in the commission of the crimes, and then through search warrants, we were able to find out the in-depth nature of their plan.

Thus, what we have done in California is to alert ourselves because the county jail system that I also manage feeds 40 percent of the State prisoners into the State system. So we have intelligence officers in our local jails as well as in the State jails, working closely with "those inmates who have leanings toward radical thinking."

Chairman COLLINS. I think there is so much we can learn from the L.A. experience, the New York experience, and from our two other expert witnesses. In many ways, our larger cities are ahead of us at the Federal level in identifying these threats and coming up with successful strategies. And that is why it disturbs me, Sheriff, to hear, because you and I have talked about this before, that DHS is still not tapping into the expertise as much as it should when it develops its own policies and procedures, and that is something we are going to need to push the Department on. I think that is so important. And I know you stand ready to help.

Senator Voinovich.

Senator VOINOVICH. Thank you. I am going to follow you. It would be very interesting to me to get your observations about what the Federal Government is or is not doing in terms of this radicalization of the Muslim population in the United States of America.

Dr. Falkenrath, you have mentioned that you see it in New York City. Mr. Simon, you have said that you see it. And the issue is: What role should the Federal Government play? Who should be playing it? And then what models are available around the country to try to bring the communities together so that we have something that we can try to replicate in other places?

Mr. BACA. If I may, Senator Voinovich, I was very pleased when you made your very strong and appropriate comments about your thoughts concerning what Muslim Americans and the radicalization issues are in the world and, of course, here. Homegrown terrorists are something that we concern ourselves with.

After the bombings in London last year, I came back from visiting with the Commissioner of Police and understood clearly that we would have to do something more than what we are doing now. So I got a hold of the Muslim American leaders in Los Angeles County, Shura Council President, which is the president of all the mosques, all mosques are nonprofits, got a hold of religious leaders. And at the time there was a fatwa that had occurred earlier, a few months earlier, from Canada and the United States of religious leaders that were Muslims, as well as scholars, who said that the Islamic belief and the Koran does not authorize and sanction suicide bombers, criminal terrorists, and the like.

We have formed, therefore, the nucleus for what is a formal nonprofit called the Muslim American Homeland Security Congress, and on the executive board are students from our local universities, women, leaders of mosques, scholars, and people who are active business people in the Muslim community. And I would say that, in deference to my friend to the left of me, I don't think that American Muslims are uninterested in participating with all of us in protecting our Nation. I think they have not organized themselves yet, and this Muslim American Homeland Security Congress is the first step through that organization. We will go to Detroit, as I mentioned. We will go to New York. We will go to Chicago. And we will go anywhere in the United States to further the regionalization of this national effort. The principal goals are to educate Muslim families as to what are the trends of radicalization within the home itself. In the London experience, many of those that were captured, their families were actually in some form of denial, in

some form of disbelief that their children were not really a part of these terrorist attacks, when, in fact, they were. So the self within the family, the educational process within the family is a very high priority of this Congress, and also its mission is to work closely with law enforcement, to work closely with local government leaders, and to not have their schools—and we have three Muslim American schools in Los Angeles County—be viewed as separatist efforts, which they are not. We have Armenian schools. We have French schools. We have various ethnic schools. And they are not viewed in the same fashion.

I can say, finally, that all of us, myself in particular, since Los Angeles County—and I do want to say Los Angeles County has 10 million people. It is the largest county in the United States, and we claim to be, like New York, the most diverse part of the United States. But we are just going to stay at a tie. And I have traveled to Jordan and met with King Abdullah. I have traveled to Pakistan and met with President Musharraf. I have traveled and met with the leaders of the justice system in Turkey, and I have seen what they have done in response to the bombing attacks that they have experienced. All three of these are Muslim nations.

What you are suggesting, I am following, and I commend you for your vision on this issue because I have heard how passionately you feel. American Muslims are patriotic to America, and that is why they are here. The radicals that are roaming about who are going to seize the moment and think they can ride themselves up on the secrecy of some kind of a cover is what we have to go after. Those are the needles in the haystack, as far as I am concerned, and that should be one of the top priorities of the Department of Homeland Security.

Senator VOINOVICH. Thank you.

Chairman COLLINS. Thank you so much for your testimony today. It was very valuable to us, and I very much appreciate your time.

The hearing record will remain open for 15 days for the submission of additional questions. All those great questions that we unfortunately do not get an opportunity to ask you today we will submit for the record.

Thank you again for sharing your expertise and for your commitment to this issue. This hearing is now adjourned.

[Whereupon, at 12:33 p.m., the Committee was adjourned.]

APPENDIX

TESTIMONY OF SECRETARY MICHAEL CHERTOFF
U.S. DEPARTMENT OF HOMELAND SECURITY
BEFORE THE SENATE COMMITTEE ON
HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS
SEPTEMBER 12, 2006

INTRODUCTION

Chairman Collins, Ranking Member Lieberman, and Members of the Committee: Thank you for the opportunity to appear before the Committee today to discuss the Department's efforts over the past three years, and the Administration's efforts since 9/11, to protect our nation against terrorist attacks while preserving our freedom and our prosperity.

Yesterday our nation observed the five year anniversary of the September 11th attacks. For most Americans, 9/11 remains a defining moment in our lives and for our nation. Even today, it is difficult to fully comprehend the devastation and loss of life flowing from the senseless murder of nearly 3,000 men, women, and children of all backgrounds and faiths, and this premeditated act of war against the United States.

9/11 was an immeasurable tragedy. But amid the horror of that day, we also witnessed tremendous courage, valor and sacrifice – embodied in first responders who gave their own lives to save those in need, and in extraordinary citizens who fought back over the skies of Pennsylvania, and in doing so became heroes.

9/11 LESSONS

Over the past five years, we have taken to heart the many lessons of 9/11, and we have acted deliberately and decisively to reduce the risk that we will ever again face another day like 9/11.

We have learned that we simply cannot be complacent in the face of terrorism. To be sure, there have been no successful terrorist attacks on U.S soil since 9/11. But the terrorists continue their plotting, as was exposed most recently this past August. Moreover, there have been terrorist attacks elsewhere against Americans, our allies, and innocent civilians, including in Bali, Madrid, and London.

Americans also have come to understand that protecting our nation involves trade-offs. We do not pursue the illusion of perfect security obtained at any price. We want security that is strong, but consistent with our freedoms, our values, and our way of life.

DHS OVERVIEW

The lesson is clear: our nation must reorient its approach to how we address 21st century threats to our homeland, and we must do so with urgency, flexibility, and resolve.

A critical part of the President's strategy to protect our nation includes fighting terrorism overseas – in Afghanistan, Iraq, and across the globe – and working with our international partners to disrupt terrorist plots and dismantle terrorist threats before they reach our own shores.

Closer to home, we must continue our work to build more integrated and effective capabilities to manage the risk to our nation. The Department of Homeland Security was created to unify national capabilities against all hazards – from hurricanes to dirty bombs and earthquakes to pandemic flu – and to work in partnership with other federal departments and agencies, state and local governments, the private sector, our international partners, and the American people.

So how do we build on our progress to date? What are our major concerns and priorities moving forward? And how do we get there?

First, it's important to make sure we are focused on the most significant risks to our homeland and that we apply our resources in the most practical way possible to prevent, protect against, and respond to both man-made and natural events.

No matter how hard we may try, we cannot eliminate every possible threat to every individual in every place at every moment. And if we could, it would be at an untenable cost to our liberty and our prosperity. Only by carefully assessing threats, vulnerabilities, and consequences, and prioritizing our resources, can we fully ensure the most practical and optimized protection for Americans and our nation.

MAJOR CONCERNS

What are we most concerned about? Our priority focus remains on those events that pose the greatest potential consequences to human life and the functioning of our society and economy. At the top of that list is the threat of weapons of mass destruction, which if used, would have shattering consequences. Preventing the introduction and use of such weapons requires our priority attention and constant vigilance.

In addition, we must continue to guard against infiltration by terrorists, including those with the capability and intent to cause significant harm to our country through multiple, high-consequence attacks on people and the economy.

Finally, we must always be mindful of the potential for homegrown acts of terrorism, including individuals who sympathize with terrorist organizations or embrace violence as a means to promote their radical agenda.

For this reason, we must not only work across federal, state and local government to prevent domestic terrorism, but we must build a new level of confidence and trust among the American Muslim community, who are critical partners in protecting our country.

ACCOMPLISHMENTS/CHALLENGES

Over the past five years, we have taken significant steps to address these and other threats by closing vulnerabilities that existed on 9/11 and creating layers of security across land, air, and sea.

Today, I would like to highlight some of the new capabilities in place protecting our nation, as well as the areas where we need to continue to press forward to build our defenses. These areas

include screening people at the border, screening cargo, protecting critical infrastructure, sharing information, and boosting emergency preparedness and response.

1. Screening People at the Border

Border Ports of Entry

First, screening people at the border. Our perimeter defense depends on keeping dangerous enemies out. Before 9/11, we had to rely on fragmented databases of biographical information to determine whether a person posed a security threat or should be allowed to enter our country. This process was often cumbersome for travelers, inefficient, and fraught with security vulnerabilities. The entry of terrorists before 9/11 tragically illustrated the cost of those vulnerabilities.

Today, we have substantially transformed screening capabilities at our international ports of entry to prevent terrorists and criminals from successfully entering our country. We have integrated our counter-terror databases and together with the State Department have dramatically enhanced visa issuance processes. As important, we have implemented US-VISIT biometric entry capabilities at 117 airports, 16 seaports, and 153 land ports of entry. Within seconds, we can positively confirm a person's identity by checking their two digital finger scans against terrorist and criminal watch lists and immigration records.

Border Security

Of course, we also have made tremendous progress securing the miles of border between our official ports of entry. This includes giving the men and women who patrol our land borders the tools, technology, and resources they need for this difficult job.

Before 9/11, our nation had 9,000 Border Patrol agents along our Southern and Northern Border. Under the President's leadership, today we have more than 12,000 Border Patrol agents, and by the end of calendar year 2008, we will have more than 18,000 agents – effectively doubling the size of the Border Patrol. Since 9/11, the Border Patrol has apprehended and sent home some six million illegal migrants attempting to cross our borders.

Before 9/11, we did not have adequate bed space to hold those we detained from countries other than Mexico, so that too often they had to be released. Today, by expanding bed space and decreasing processing times, we have essentially ended this practice of catch and release at the southern border. Now, virtually all illegal migrants caught at the border are detained and removed. The result: for the first time, we are seeing a seasonal decline in the number of illegal migrants attempting to cross our nation's southern border.

Today, under the Secure Border Initiative, we are substantially implementing new technology, staff, and tactical infrastructure at the border. We still have much work to do to secure our borders, but we have made significant progress on this important front and we have developed a strategy that will allow us to achieve even greater control of our borders over the next two years.

Passenger Data

So what are the areas where we must do more to identify and screen those that may pose an evil intent?

As the recent London airline threat emphasized, we must be able to determine who is on-board an aircraft and whether that individual is on a watch list before the plane leaves for the United States. Under our current arrangement, we vet this passenger information a full fifteen minutes after the plane takes off. That is simply too late.

Our goal is to implement a system that requires airlines to transmit passenger information well in advance of departure. This will give us the necessary time to check passenger names and coordinate with airlines and foreign law enforcement to interdict a suspicious person at the departure airport or prevent that person from boarding a plane bound for the U.S.

Apart from known terrorist threats, we also need to be able to identify unknown terrorist threats – that is, people who don't appear on any watch list or in criminal databases. One of our most valuable tools to do this is actually at our fingertips – the Passenger Name Record (PNR) data routinely collected by the travel industry when an international traveler makes an airline reservation or purchases an airline ticket.

Over the coming months, I look forward to working with the European Union to examine options to share PNR data among law enforcement agencies while ensuring adherence to appropriate privacy safeguards. We must do so quickly, but also ensure that transatlantic flights continue.

Secure Documents

A second area where we must accelerate efforts is the development of secure travel and identification documents. We must develop standard, secure credentials that give us a high degree of confidence that an individual is not using false or stolen documents to enter our country or access our transportation systems or sensitive critical infrastructure.

A number of initiatives now underway will allow us to do this. Under the Western Hemisphere Travel Initiative, we are working together with the Department of State to develop a secure credential for individuals traveling between the United States, and Canada and Mexico. This card will be wallet-sized, contain security features, and allow real-time security checks at land border crossings and certain water border crossings.

We are also working with states to develop standards for secure driver's licenses under the REAL ID Act. Driver's licenses are one the most common forms of identification used in our country. We must have clear guidelines for how these documents are produced, who gets them, and what security features they must contain.

Five years after 9/11, some are beginning to complain that these measures are not necessary. I disagree. They are as necessary now as they were five years ago. Of course, we must implement secure document requirements as efficiently and economically as possible. But at the end of the day, we must have the will to implement these measures if we are going to heed the lessons of 9/11 and reduce the risks for the future. Documents such as these will not only increase security, but speed processing for travelers.

Fingerprint Collection

We also need to make sure we are able to exploit combined law enforcement fingerprint databases to our greatest advantage. Critical to this is moving from a two fingerprint collection system to a 10 fingerprint system for visitors to the United States. Taking all 10 fingerprints from travelers will allow us to do a more comprehensive identification check and a more thorough search of existing criminal databases.

The State Department will deploy new 10-print devices at U.S. visa-issuing posts overseas. We will also begin deployment of these same devices to our border ports of entry to electronically collect 10 flat fingerprints for visitors not previously enrolled in federal fingerprint databases.

2. Screening Cargo/Preventing WMD

Let me now talk about what we've done since 9/11 to monitor the cargo entering our nation and prevent the entry of Weapons of Mass Destruction – and what we want to achieve in the future.

Before 9/11, we screened very few cargo containers entering our ports or crossing our borders for terrorist weapons. We did not have the ability to examine that cargo overseas before it left a foreign port for the United States. Nor did we have adequate automated scanning for radiation, next generation detection technology, or a formal partnership with the private sector to increase security in privately owned supply chain operations.

Today, all of this has changed. Through our National Targeting Center, every shipping container entering the United States is assessed for risk, and high-risk containers are inspected. Moreover, under the Container Security Initiative, U.S. inspectors stationed at 44 overseas ports now screen 80 percent of the cargo bound for the United States before it reaches our shores. By the end of this year, those inspectors will screen cargo at 50 foreign ports.

In addition, we have deployed hundreds of Radiation Portal Monitors and thousands of hand-held radiation detection devices domestically to protect against radiological and nuclear threats. As a result of these capabilities, we will screen nearly 80 percent of maritime container cargo arriving at U.S. ports for radiation by the end of this year. Finally, almost 6,000 companies have joined our Customs Trade Partnership Against Terrorism to voluntarily take steps to enhance security in their supply chain operations.

In all, the federal government has dedicated nearly $10 billion to port security since 2004, including the efforts of the Coast Guard, Customs and Border Protection, and the research and development efforts of our Domestic Nuclear Detection Office, and the Department of Energy. These actions have not only increased security, but they support the free flow of commerce and trade essential to our economy.

Biological Countermeasures

Since 9/11, we also have significantly strengthened the nation's defenses against biological threats by developing and deploying a network of biological sensors; establishing new facilities to monitor, test and detect potential biological threats; and utilizing new risk assessment tools to inform investments and potential threats.

In partnership with the Environmental Protection Agency (EPA) and the Department of Health and Human Services (HHS), we have deployed the first ever bioaerosol monitoring system to more than 30 major metropolitan areas in order to provide early warning of an attack and enable quick and accurate response. The BioWatch system is currently undergoing expansion in the top threat cities to enable detection of smaller amounts of bio-agents, better define the affected areas in the event of a release, and provide increased coverage of critical facilities such as transportation networks.

We also have established the National Biosurveillance Integration System, a 24 hour operation designed to provide early recognition of biohazards of potential national significance and to form a common operating picture through all-source reporting relating to all types of public health threats. And in partnership with the Federal Bureau of Investigation, we have established the National BioForensics Analysis Center (NBFAC) to conduct and facilitate forensic analysis and interpretation of materials recovered following a biological attack.

Radiological Screening

These are major advances in protecting our nation against Weapons of Mass Destruction. But in the future, we must continue to develop and deploy systems to prevent and detect nuclear or radiological attacks in the United States. To accomplish this goal, we will do a number of things.

First, we will complete the deployment of Radiation Portal Monitors to all of our southern and major northern land border crossings and to every major seaport by the end of next year. We will also make substantial investments in next generation detection technology, including $1.15 billion for the Advanced Spectroscopic Portal program to enhance detection capabilities for radiological and nuclear materials.

Secure Freight

To expand protection of the vast amount of cargo that moves throughout the global supply chain, we are also increasing the extent and depth of information we will be able to use to draw a more detailed picture of the movement of a container as it travels through the supply chain. Implementing this Secure Freight program over the next two years will require considerable work with our interagency and overseas partners, and international organizations. We look forward to working at home and overseas to implement this new vision for cargo security.

Securing the Cities

Finally, by the end of 2008, we will complete the first phase of a "Securing the Cities" program in New York City to conduct nuclear and radiological scanning on the principal pathways into the city – over land, over water, and underground. In addition, we anticipate two additional cities will be part of the "Securing the Cities" program. And we will conduct radiological and nuclear preventive training for 300 state and local officials this fiscal year and quadruple that number by the end of next year.

3. Infrastructure Protection

Let me turn now to infrastructure protection. One major area of focus for the Department has been protecting our nation's transportation systems in partnership with state and local governments and the private sector.

Transportation

Let me begin with our aviation system. Before 9/11, we did not have secure cockpit doors. We did not have a federalized screener workforce trained to detect bomb components and detonation devices. We did not have thousands of Federal Air Marshals aboard aircraft, protecting travelers every day all over the world. We did not have armed pilots authorized to defend the cockpit. We did not have 100 percent screening of all passenger baggage. Nor did we have thousands of Explosive Detection System machines scanning passengers and baggage at airports nationwide.

Today, more than a dozen layers of security are now in place and create a protective fabric of security that keeps hundreds of thousands of air travelers safe and secure every day. Of course, we continue to look for ways to stay ahead of changing terrorist tactics. But we have laid the foundation for the future of our aviation security efforts for years to come.

Of course, our efforts are not confined to aviation. In the rail and mass transit sectors, we've invested in new technology, rider education and awareness programs, sensors and video cameras, and law enforcement surge capabilities, including trained canine teams.

Since 9/11, we also have performed thousands of vulnerability assessments and reviewed thousands of security plans for privately owned infrastructure across the country – including transportation assets, seaports, and chemical facilities. And we have established new information-sharing portals with the private sector to warn of threats and to recommend protective measures.

In all, since 2002, we have provided more than $1.1 billion in risk-based grants specifically for the protection of critical infrastructure. This past June, we also finalized the National Infrastructure Protection Plan, our over-arching playbook for protecting our nation's critical infrastructure.

Chemical Security

Of course, we know that the vast majority of critical infrastructure in our country is owned and maintained by the private sector. The government alone cannot protect these critical assets and key resources. Only by working together can we enhance protection.

One area where we continue to face a challenge is in developing a risk-based regulatory structure for our nation's chemical plants and facilities.

Since 9/11, most chemical companies have been good corporate citizens – voluntarily taking steps to improve security in their operations and facilities. But not all companies have increased security to an appropriate level – and those companies put everyone else at risk.

We must develop a balanced, common-sense approach for protecting chemical facilities across our country – and their surrounding communities – without destroying the businesses we are trying to protect.

But we cannot do so unless our Department has the authority to set standards, develop risk-based approach for different kinds of facilities, validate security measures, and insist on compliance.

That is why today I want to urge Congress to pass chemical security legislation that will allow us to partner with industry to develop a clear way forward that includes creating a tiered structure for assessing risk and a clear program to ensure compliance.

4. Intelligence

As we know, the best way to protect against a terrorist attack is to prevent it from happening – and intelligence is our most effective means of defeating terrorist plots before they become operational.

Under the leadership of President Bush, the Administration has integrated intelligence collection and analysis across all the elements of the intelligence community under the Director of National Intelligence and the Program Manager Information Sharing Environment.

At the Department of Homeland Security, we have a strengthened and unified intelligence office led by a veteran intelligence official. And through our Homeland Security Information Network, thousands of state and local participants share information every day on threats and incidents within their communities.

Fusion Centers

In the future, we intend to expand these valuable partnerships even further by substantially increasing federal participation in state and local fusion centers across our country as part of an interagency effort to better share intelligence with state and local governments. DHS intelligence personnel already work side-by-side with their federal, state and local counterparts at fusion centers in New York, California, Georgia, Louisiana, and Maryland. Our goal is a two-way flow, with every level of government pooling intelligence.

By the end of 2008, working with our other federal partners, our goal is to have intelligence and operations personnel at every state and major metropolitan fusion center in the United States, sitting in the same room, sharing and analyzing information and intelligence in real time.

5. Preparedness/Response

Finally, we know that some threats we will not be able to prevent – specifically those created by Mother Nature. As an all-hazards Department, we must be prepared to respond to acts of terrorism as well as acts of nature, including acts of such catastrophic proportion that federal intervention is required before, during, and after the storm or event.

Since 9/11, we have re-tooled and re-fashioned the Federal Emergency Management Agency, giving this vital agency new and experienced leadership, enhanced, real-time tracking

capabilities for emergency supplies, and robust emergency communications systems. We have pre-designated and pre-positioned Federal leadership in hurricane zones to work together with state and local officials, and we have forged a stronger partnership with the Department of Defense to ensure joint training and operations.

To respond to no-notice or short notice events, our operational agencies – including the Coast Guard, Transportation Security Administration and its Federal Air Marshal Service, Immigration and Customs Enforcement, Customs and Border Protection, and the Secret Service – have created, or are now creating, "adaptive force structures" that will rapidly deploy to an incident or disaster zone to provide an immediate surge capability and greater unity of effort.

The emergency management community now operates under a new, comprehensive National Response Plan and a National Incident Management System. And we have created new preparedness tools for individuals and businesses under the Ready campaign and new community-based training programs under Citizen Corps.

Interoperable Communications

But despite this progress, we still have more to do to fully realize the potential of our Department to integrate the full range of national capabilities. And one area in particular that requires continued action and attention across all levels of government is interoperable communications.

On 9/11, hundreds of first responders couldn't communicate with each other because their radios were incompatible. This not only slowed the response and increased confusion, but it cost lives. As a nation, we simply can't let that happen again.

Today, we have achieved interoperability at the command level in 10 of the highest-threat urban areas through our RapidCom program. Achieving interoperability continues to be one of seven National Priorities under the Interim National Preparedness Goal. As a result, state and local governments, and first responders, have spent about $2.1 billion of Federal grant assistance since 2003 for interoperable communications equipment, planning, training, and exercises.

In addition, we completed a National Interoperability Baseline Survey to assess the capacity for communications interoperability among law enforcement, fire, and emergency medical service first responders in all 50 states and D.C. But more needs to be done.

By the end of this year, we will have a clear plan in place for completing command-level interoperability among police, firefighters, and emergency medical service providers in each of the states and at least 75 urban areas.

Of course, we can only do so much at the Federal level to resolve differences at the state and local level. We can develop standard operating procedures, recommend technology, and lead training and exercises, but local governments ultimately use the equipment and execute their plans.

In the coming months, we will turn to our state and local partners for guidance, for answers, and ultimately, for results.

CONCLUSION

Five years ago, on the beautiful, clear morning of September 11th, 2001, the men and women that went to work at the World Trade Center and the Pentagon, and those that boarded United flights 93 and 175, and American Airlines flights 11 and 77, did not know the tragic fate that lay before them.

The victims of 9/11 were sons, daughters, mothers, fathers, sisters, and brothers. They had dreams, they had plans for their future, and they had families that loved them. And in the span of a few hours, their lives – and the lives of thousands of people who knew them – were shattered, along with the belief that our homeland was immune to the danger of international terrorism.

Today, our nation is at war. We are fighting an enemy who will not rest until its dark vision of the future is achieved. We cannot relent from this struggle. We cannot become complacent. And we cannot forget what happened on that September morning five years ago.

Over the past three years, we have built a department whose mission is to work on behalf of the American people – and on behalf of the victims of 9/11 – to prevent, protect against, and respond to threats to our homeland. For the 185,000 men and women of DHS, this is a mission we are proud to undertake every day – at our borders, across our skies, and over land and sea.

The steps we have taken since 9/11 have made our nation safer, they have made our nation stronger, and they have made our nation more resilient – economically resilient and resilient in spirit. I appreciate the support of this Committee and all Members of Congress as we continue to build the capabilities of our department and continue to protect our nation in the months and years to come.

SENATE COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

TESTIMONY OF
LEROY D. BACA, SHERIFF
LOS ANGELES COUNTY
September 12, 2006

CALIFORNIA IS A FORMAL MUTUAL AID STATE (Circa 1950)

While our nation's efforts to deal with terrorism are beginning to shift to prevention as a primary goal, over the past five years, our focus has been on our ability to respond to an attack. Because of our frequent experience with disasters, the State of California has a very structured organization for emergency and disaster management. The Standardized Emergency Management System (SEMS) is required by California Government Code §8607(a) for managing response to multi-agency and multi-jurisdiction emergencies in the State. SEMS incorporates the use of the Incident Command System (ICS), the Master Mutual Aid Agreement, existing discipline specific mutual aid, the operational area concept, and multi-agency or inter-agency coordination. SEMS helps unify all elements of California's emergency management organization into a single integrated system. This is the framework on which the National Incident Management System (NIMS) is based.

CALIFORNIA SHERIFFS ARE MUTUAL AID COORDINATORS

Mutual aid response within California is based on four governmental levels of increasingly justifiable mutual aid support. These levels delineate cities (or other similar local jurisdictions), operational areas (counties), mutual aid regions, and the State. To facilitate coordination of mutual aid, the State is geographically divided into seven law enforcement mutual aid regions, comprised of multiple operational areas. The operational area is a composite of its political subdivisions, i.e., municipalities, contract cities, special districts, and county agencies. Each region has a county sheriff designated as the Law Enforcement Mutual Aid (LEMA) coordinator. I act as that coordinator for Region I, which is comprised of Los Angeles and Orange Counties (13 million people). In addition, during a declared emergency, I am designated as the Director of Emergency Operations for the Los Angeles Operational Area, which includes 88 cities and unincorporated areas spread over more than 4,000 square miles.

TERRORISM EARLY WARNING (TEW) GROUP SYSTEM PRIOR TO 9/11

Although more than five years have elapsed since the tragedy of 9/11, the Los Angeles County Sheriff's Department remains committed to institutionalizing the lessons learned that day. Together with our federal, state and local partners,

we are aggressively pursuing new ways to integrate our disparate agencies into a seamless network of information sharing cooperatives. To understand where the Los Angeles County Sheriff's Department is headed, there must be an understanding of where we have been.

In 1996, the Terrorism Early Warning (TEW) Group was developed by the Sheriff's Department in order to analyze trends and potentials for a terror attack within Los Angeles County. The TEW now employs subject matter experts from law enforcement, the fire service, public health, academia and the military all working together to ensure the safety of Los Angeles County residents. Representatives from the FBI and the Department of Homeland Security also work within the TEW to produce high-quality, analytical products that are provided to decision makers covering a variety of subjects related to terrorism.

JOINT REGIONAL INTELLIGENCE CENTER OF SOUTHERN CALIFORNIA

Recognizing the value of cooperation between federal, state and local agencies, leaders from the FBI, United States Attorney General's Office, State Office of Homeland Security, Los Angeles Police Department, and Los Angeles County Sheriff's Department decided more than two years ago to join together and create a model for intelligence fusion centers. The vision became reality in July of this year with the grand opening of the Los Angeles Joint Regional Intelligence Center (JRIC). Using analytical processes developed by the TEW, analysts from a variety of agencies and disciplines create an expansive view of trends and potentials that could indicate a pending terrorist attack. The United States Department of Homeland Security is also present in the JRIC, and components of that department such as Customs and Border Protection, Immigration and Customs Enforcement, Transportation Security Agency, and the Coast Guard have been encouraged to contribute personnel to the JRIC. These agencies possess critical information that must be synthesized with local products to provide the clearest possible forecast of potential threats. I continue to strongly encourage the participation of any public agency involved in issues of Homeland Security with its local TEW or other fusion center. The collaboration between local and federal partners for making critical decisions pertaining to homeland security helps to overcome the traditional bureaucratic inertia in the field of intelligence sharing.

TERRORISM LIAISON OFFICERS

The State of California realized the value of such intelligence cooperatives and funded four Regional Terrorism Threat Assessment Centers (RTTAC). The Los Angeles JRIC is the model for RTTAC development in California and is being replicated in the other areas.

One of the successful initiatives operating out of the JRIC is the Terrorism Liaison Officer (TLO) program. Originated shortly after 9/11, this program seeks

to create a network of trusted agents within each law enforcement, fire and health agency in Los Angeles County that provides the vehicle to exchange valuable information to and from the JRIC. As a result, local police officers, firefighters and health professionals have generated numerous leads of "investigative interest." This level of intelligence-based connectivity between field personnel is unprecedented and has enhanced the level of situational awareness in the region. Information provided by the TLO network contributes to the development of intelligence that is disseminated weekly to the executive staff of participating agencies, field operators, and line personnel.

FORMAL PRIVATE SECTOR OUTREACH AND PARTNERSHIP

Outreach from the JRIC is not limited to public safety personnel. Shortly after 9/11, I developed the Homeland Security Advisory Council (HSAC) in an effort to network corporate leaders with the work of the TEW/JRIC. HSAC is comprised of senior corporate leaders from Los Angeles and Orange Counties, and is chaired by Mr. Marc Nathanson, Founder of Falcon Cable Corp. Members of the HSAC provide technical, political and financial support to our counter-terrorism mission. Through their large sphere of influence, they also provide connectivity to corporate security departments who have shared information of investigative interest to the TEW and JRIC. In order to expand this capability nationally, the HSAC has also affiliated with the Business Executives for National Security (BENS). Integrating the private sector into our intelligence process led to the creation of Infrastructure Liaison Officers (ILO). The ILO program further expands the network of trusted agents to include people dedicated to critical infrastructure protection (CIP). This addition to our intelligence process creates a comprehensive network that provides a better opportunity for the prevention, disruption or mitigation of a terrorist attack.

FORMAL MUSLIM AMERICAN OUTREACH AND PARTNERSHIP

Another key component to our overall strategy is our connection to the Muslim community through the creation of the Muslim American Homeland Security Congress (MAHSC). Consisting of respected leaders from Muslim organizations within Southern California, their mission is to foster communication, education and mutual respect between law enforcement and the Muslim community. Programs such as the HSAC and MAHSC are reflective of our belief that Homeland Security is not an issue that can be resolved through traditional police practices.

THE NEXT FIVE YEARS

The challenges of the next five years are many and varied. Essential above all is to continue to build the relationships among all entities (local, national and international) involved in the Homeland Security mission. Knowing that homeland security is truly a global enterprise, with the help of local consul

generals, members of the Los Angeles County Sheriff's Department have traveled to Russia, Pakistan, Jordan, Israel, France, Germany and Great Britain to educate themselves on "best practices" in prevention, disruption and response to terrorist activity.

For the next five years, we need to fine tune the aforementioned accomplishments and do the following:

1. Communications

   - The interoperability gaps for police, fire and medical responders must be closed.

   - Intelligence must be shared vertically and horizontally across jurisdictions for analysis, investigative and operational purposes.

2. Technology

   - Surveillance technology needs additional development and standards.

   - Detection technology for chemical, biological and radiological applications need additional development.

   - National technology resources need further logistical development for regional/national application (shared classified technology), i.e., the Department of Defense and the National Intelligence Community has equipment local police do not have.

   - Research and development of new technology should be jointly managed to avoid wasteful duplication. This should be managed by a national board of volunteer federal, state and local intelligence and first responder experts.

3. Joint Forces Terrorist Training Center

   - Develop three or more training centers on terrorism for federal, state and local first responders and intelligence first preventers of terrorist acts. The California National Guard and California Mutual Aid Region I (Los Angeles and Orange Counties) are currently developing this proposal.

4. International cooperation, training, best practices, and personnel exchanges should be expanded. Current plans are underway to have training occur in Paris, France at the Interpol Headquarters led by cities and countries that have experienced a terrorist attack.

5. Continue to fund and develop the National Terrorism Early Warning Resource Center that partners with local and state law enforcement. There are currently 26 local TEW operations in the nation. The long-range vision and effort is to link more than 50 TEWs across the country with other local and state fusion centers such as JRIC (Joint Regional Intelligence Center).

6. The Department of Homeland Security's major policies should be developed in partnership with selected experienced local, state and federal law enforcement leaders in deciding financial, operational, and training policies. The UASI grant program is one example.

As the elected Chief Law Enforcement Officer of America's largest county of 10 million people, I thank you for the opportunity to present my testimony to you.

RICHARD A. FALKENRATH
DEPUTY COMMISSIONER FOR COUNTERTERRORISM
NEW YORK POLICE DEPARTMENT

PREPARED STATEMENT OF TESTIMONY
BEFORE THE
COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS
UNITED STATES SENATE

SEPTEMBER 12, 2006

Good morning, Madam Chairman, Senator Lieberman, and Members of the Committee. I am honored to have this opportunity to appear before your committee one day after the five-year anniversary of the terrorist attacks of September 11, 2001.

For the record, my name is Richard A. Falkenrath. I am the Deputy Commissioner of Counterterrorism in the New York Police Department. Prior to joining the NYPD, I was the Stephen and Barbara Friedman Fellow at the Brookings Institution. From 2001 until 2004, I served on the White House staff, first as Director for Proliferation Strategy on the National Security Council staff; then as Special Assistant to the President and Senior Director for Policy and Plans within the Office of Homeland Security; and finally, as Deputy Assistant to the President and Deputy Homeland Security Advisor. Before government service, I was an Assistant Professor of Public Policy at the John F. Kennedy School of Government, Harvard University.

I will begin this testimony by giving you a brief overview of the New York Police Department's counterterrorism program. I will then summarize for you the Department's present view of the terrorist threat – globally, nationally, and to New York City. I will conclude prescriptively by making a set of recommendations on how the federal government can do a better job securing the homeland in general and New York City in particular.

I speak to you today not in my personal capacity but as a representative of the NYPD. Nonetheless, I may from time to time provide a perspective that derives from my experience as a former academic specialist on homeland security and former federal homeland security official.

I. The NYPD Counterterrorism Program

The NYPD is charged with the protection of New York City. With a population of over 8.1 million and an area of 321 square miles, New York is the largest city in the United States. New York is also the most densely populated major city in North America as

well as one of the most diverse: an estimated 40 percent of the population of New York City is foreign born. The New York metropolitan area has a population of 18.7 million, making it one of the largest urban areas in the world. New York City is an international center for business, finance, media, culture, diplomacy, tourism, and travel. In 2004, the gross metropolitan product of the New York urban area was estimated at $901.3 billion, a level greater than all but about a dozen countries in the world.

With a staff of over 52,000 people and an annual budget of $3.8 billion, the New York Police Department is the largest public safety agency in the United States and one of the largest police departments in the world. (For comparison, the NYPD is larger than the U.S. Coast Guard and more than twice the size of the Federal Bureau of Investigation; at the federal level, only the Army, Navy, Air Force, and Marine Corps are larger.) Over 1,200 NYPD personnel are members of the National Guard or the Reserves; more than 800 have served or are serving in Iraq.

Since the early 1990's, the New York Police Department has been a national leader in crime reduction. According to the Federal Bureau of Investigation's uniform crime reports, New York City is now the safest big city in the United States – an astounding achievement when one recalls the crime epidemics that gripped the City in the 1970's and 1980's.

Every American remembers the heroism and sacrifice of New York City's first responders – from the Fire Department of New York, the Port Authority Police Department, the NYPD, and many other agencies on September 11, 2001. I can claim no credit for their heroism and sacrifice – at the time of the attacks, I was working in the relative safety of the White House – but I serve now with the knowledge that my present-day colleagues lost family and friends that day and risked their own lives, and will do so again if we are attacked once more.

Needless to say, since the terrorist attacks of September 11, 2001, the NYPD has enhanced its counterterrorism program in a manner that is unique in this country. The

New York Police Department has made the defense against the terrorist threat its number one priority. Immediately after his appointment, Police Commissioner Raymond W. Kelly created the NYPD's Counterterrorism Bureau, which I now have the privilege to lead. My two predecessors are two men with decades of distinguished national-security experience at the federal level: retired Marine Corps Lieutenant General Frank Libutti, the former Commanding General of Marine Forces Pacific; and Ambassador Michael Sheehan, a member of the National Security Council staff under three presidents and the Department of State's former Ambassador-at-Large for Counterterrorism.

Commissioner Kelly has also dramatically expanded the Department's Intelligence Division. The Deputy Commissioner for Intelligence is David Cohen, a 35-year veteran of the Central Intelligence Agency and its former Deputy Director of Operations. The NYPD's intelligence program is nimble, innovative, and unique in the United States. By combining select elements of CIA tradecraft with tried-and-true law enforcement techniques, and utilizing the New York Police Department's legal authority, the intelligence program has produced remarkable results. One of the benefits of this program came to light in August 2004, when the Police Department foiled a plan by two home-grown Muslim extremists to bomb the Herald Square subway station in midtown Manhattan. The NYPD arrested those suspects just a week before the Republican National Convention with the help of a confidential informant the Intelligence Division had developed in the community.

In the words of FBI Director Robert Mueller, the NYPD's Counterterrorism Bureau and revamped Intelligence Division are "models for the nation."

All together, the New York Police Department dedicates more than 1,000 officers, and allocates roughly $200 million dollars annually, to the counterterrorism mission. Over 100 NYPD detectives – all of whom report to me – are assigned to New York's Joint Terrorism Task Force (JTTF). Hundreds of NYPD personnel have been granted security clearances by federal agencies. NYPD detectives frequently travel to the

Guantanamo Bay facility and other locations abroad to interview detainees about ongoing cases. The Department has roughly 275 certified interpreters of 45 different foreign languages – including Urdu, Hindi, Pashtu, and Arabic – whose specialized abilities have been used by federal national security agencies on numerous occasions.

The NYPD has implemented a wide range of specific counterterrorism initiatives and programs, including the following.

Counterterrorism Field Operations. In 2003, the NYPD implemented a comprehensive security plan known as Operation Atlas that incorporates highly visible deployments throughout the city. These are designed to disrupt terrorist planning and surveillance operations and include Critical Response Vehicle (CRV) surges, Hercules Team deployments, Transit Order Maintenance Sweeps (TOMS), and Subway Explosive Trace Detection checkpoints.

CRV operations bring patrol vehicles from each of the 76 precincts in New York City to a central location, allowing for a show of force and deployment to high-threat, high-value target locations across the City. Our Hercules deployments are comprised of mobile teams of heavy weapons-equipped personnel who patrol at sensitive locations throughout the City. TOMS consist of teams of uniformed officers that sweep trains for suspicious persons or packages. These sweeps are sometimes conducted in conjunction with explosives trace detection screening operations that can detect explosives residue on items people are carrying into the subway system.

Threat and Vulnerability Reduction. The NYPD created a threat reduction and infrastructure protection program. Critical infrastructure is divided into five categories, and a team of investigators covers each one. These officers visit facilities throughout the City, identify vulnerabilities, and develop comprehensive protection plans with site managers. Members of the Counter Terrorism Bureau have conducted hundreds of threat and vulnerability assessments of strategic and high-visibility sites. The goal of

these assessments is to work with the private sector and other city agencies to improve the security of their facilities against terrorist attacks.

International Liaisons. In addition to enhancing our domestic law enforcement partnerships, the NYPD has established an international intelligence liaison program. Currently, the NYPD has ten officers assigned to eight foreign countries. Our goal is three-fold. First, we are seeking to uncover any information pointing to another terrorist attack against New York City. Second, we are seeking to uncover any terrorists or their supporters residing in the New York metropolitan area. Third, we are developing information on the terrorists' tactics and methods and the best practices we can use to defeat them. We are also developing our own direct relationships with foreign law enforcement agencies for the specific purpose of gathering terrorist-related information that is generated overseas.

Detectives have covered a number of international terrorist acts, including the March 2004 Madrid attack, the July 2005 London bombings, and the recent incident in Mumbai, India. The intelligence they collect and transmit back to the Department immediately impacts the deployment of personnel and resources to ensure proper protective measures are in place throughout the City.

Intelligence Analysis. The Department has hired a cadre of trained civilian intelligence analysts to take raw information gathered from informants and undercover agents in the field and translate it into valuable, real-time reporting for our commanders. These analysts work to ensure a steady flow of intelligence on the terrorist threat. They routinely provide Terrorism Awareness Bulletins to every precinct and command in the City. These are read at every roll-call and posted conspicuously for all officers to review.

CBRN Defense. The Department has deployed a variety of different teams that specialize in response to chemical, biological, and radiological events throughout the City. We established a medical team to help protect our officers from chemical,

biological, and radiological attacks. The Department has distributed personal protective equipment and sophisticated detection equipment to members of the Department, including sensors to detect the presence of radioactive material and personal dosimeters. In addition, the Department established a medical directorate within the Counter Terrorism Bureau to help us protect our officers and to advise us on our preparations for responding to a chemical, biological, or radiological attack.

The NYPD has also acquired approximately 700 hand-held gamma monitors, otherwise known as radiation pagers, and 120 gamma neutron detectors to detect potential radiological weapons of mass destruction. These pagers have been distributed throughout the Department. Over 200 pagers have been designated for precincts, with the requirement that every Sergeant on patrol carry one at all times while on duty.

Radiation pagers have also been issued to our Special Operations Division, our patrol task forces, the Shea and Yankee Stadium details, members of the service stationed at ferry terminals, our headquarters security unit, and other commands. The Housing and Transit Bureaus have distributed pagers among key patrol posts. In addition, advanced gamma detectors and Geiger counters have been assigned to other specialized units such as the Emergency Service Unit and the Bomb Squad. The Department continues to seek out and acquire new technologies to aid us in the war on terror. In the future, we plan to procure additional nuclear, biological, and chemical detection and monitoring devices.

Outreach to the Private Sector. Under Operation Nexus, members of the NYPD Intelligence Division meet with small business owners and suppliers throughout the city who might unwittingly be used to provide material support to terrorists. Our goal is to increase their counterterrorism awareness. We ask them to report anomalies in purchases of goods and specialized rental equipment to our citywide counterterrorism hotline.

In July 2005, the NYPD launched a new initiative with the private security industry in New York called "NYPD Shield." We have created a comprehensive program website featuring training materials and threat updates, and we have offered detailed briefings to a number of private sector industries.

We exchange threat information daily with the city's corporate and institutional security directors though an instant messaging system. NYPD has also held briefing sessions for various segments of the public who may come in contact with terrorist plotters.

Counterterrorism Inspectors. We have assigned a senior officer responsible for overseeing counterterrorism initiatives at the rank of Inspector (the NYPD equivalent of a Colonel) to each patrol borough. These executives are responsible for all counterterrorism issues within the borough command. They also ensure that all counterterrorism training and equipment mandates are complied with by every precinct within the borough command.

Lower Manhattan Security Initiative. The Lower Manhattan Security Initiative (LMSI) is an in-depth, intelligence-driven counterterrorism plan designed to improve the security of lower Manhattan, perhaps the single most important center in the global financial system. When fully implemented, Lower Manhattan will be one of the most target-hardened areas in the nation. This initiative will include closed circuit surveillance cameras and License Plate Recognition readers (LPRs) on every bridge and tunnel coming into and leaving lower Manhattan. In addition, steel barriers will be used to block access to sensitive streets and locations. Mobile LPRs will be mounted on helicopters and deployed in non-descript vehicles to aid in the tracking and interdiction of suspect vehicles, and upwards of 1,000 officers will be dispatched from a central coordination center. This will significantly enhance our response capacity to any major incident affecting lower Manhattan.

The Department has engaged in an extensive collaboration with the New York Stock Exchange and downtown business leaders. The area around the Exchange is the

subject of 24-hour police presence. We also established vehicle checkpoints at seven major intersections leading into the Exchange. Each is monitored by Stock Exchange security officers trained by the NYPD. Each checkpoint is outfitted with Police Department-recommended equipment including Department of State-rated vehicle barriers configured to deter truck bombs, explosives screening points, and ballistic-resistant guard booths.

Counterterrorism Training. In the aftermath of 9/11, the NYPD developed a broad counterterrorism training curriculum for all ranks within the Department. This curriculum includes instructional courses based upon existing and developing trends in target selection and attack methodologies, using our broad experiences as a law enforcement agency in intelligence collection and analysis; force protection; target hardening; countersurveillance; and terrorist tradecraft. Recognizing the critical need to share information with all those engaged in the war on terror, the NYPD established a regional counterterrorism training center in 2002. This center provides training to both our own members and our local law enforcement and public safety partners in recognition of the fact that terrorists do not recognize jurisdictional and geographic boundaries.

This regional training center provides training to members of the New York City Fire Department; the Metropolitan Transportation Authority Police Department; the New York State Police; the Nassau, Suffolk, Westchester, and Rockland County Police; as well as police departments and other public safety agencies from New Jersey, Connecticut, Maryland, Minnesota, Virginia, and even Canada. We also routinely train members of the Federal Protective Service, U.S. Coast Guard and Park Police. We have brought in dozens of private security professionals from hotels, banks, and other institutions to train them in ways to better protect their facilities. In all, over 130,000 training days have been provided by the regional training center since early 2002.

The Hazardous Materials Operations course was implemented in November 2003. It has been certified by the DHS Office of Grants and Training and been delivered to in excess of 15,000 members of the Department. In addition, a one-day Counterterrorism

Awareness for the Law Enforcement Professional course, a two-day Advanced Explosive Trace Detection, a three-day Vehicle-Borne Improvised Explosive Device (VBIED) / Checkpoint Operations, and a ten-day Tradecraft for Asset Handlers course have been developed and submitted for certification by the DHS Office of Grants and Training.

NYPD has also provided training to all of our uniformed personnel in the new Citywide Incident Management System (CIMS). The system provides for a command structure that allows the Department to work seamlessly with other first responders, as ideally envisioned in the National Response Plan.

The result of our significant training activity is that New York City has never been better prepared to defend itself from a terrorist threat. These preparations, however, come at a steep price: about $178 million per year to maintain our daily counterterrorism and intelligence activities. I want to emphasize: these are ongoing operational costs to defend the city.

The Department needs the ability to self-certify the training courses we regularly and expertly deliver. We find particularly onerous the DHS requirement to obtain DHS certification of our training courses before federal grant funding may be used to provide this training to our members. This requirement delays our training, most of which is provided on overtime, so as to avoid any reductions in our operational patrol strength.

Exercises. The NYPD routinely conducts counterterrorism mobilization drills involving members of our patrol and special task forces to discern who should, and who should not, respond to major disaster scenes. These drills are conducted at high visibility sites. In addition, we consistently run tabletop exercises for our senior executives to practice our decision-making in response to mock attacks.

We conduct daily exercises throughout the City in responding to a terrorist attack. This constant training and drilling paid off during the blackout of 2003, when the Department

was quickly mobilized to protect the city against the potential for disorder. Given our high state of preparedness, few arrests were necessary and disruptions were kept to a minimum.

Special Events and Security. The NYPD routinely handles security and provides comprehensive police services at hundreds of large major public events annually. These include, for example, the annual United Nations General Assembly; dozens of parades; street fairs; demonstrations; and high-profile/high-threat dignitary visits. The Republican National Convention of 2004, a national special security event, was one such major undertaking that demanded a great deal of planning and staffing resources on our part. The Department's size and experience allows us to satisfy these additional security needs while maintaining the same high level of police protection and service throughout the City.

II. The Terrorist Threat – Globally, Nationally, and to New York City

Terrorism is not an abstraction to New York City. Consider the following 18 events from the recent past:

1. NOVEMBER 5, 1990: El Sayyid Nosair shot Jewish Defense League leader Meir Kahane in front of the Marriot East Side Hotel in Manhattan. Nosair would later become a co-conspirator with the "blind sheikh," Omar Abdul Rahman, in a plot to destroy New York City tunnels and bridges.

2. FEBRUARY 26, 1993: New York City sustained the first terrorist attack on the World Trade Center; six innocent people were killed.

3. JUNE 1993: An al-Qaeda plot to destroy the Holland Tunnel, the Lincoln Tunnel, the George Washington Bridge, and the United Nations Headquarters was uncovered, and the plotters successfully prosecuted.

4. MARCH 1, 1994: Rashid Baz, a Palestinian angered by an Orthodox Jew's attack on a Muslim holy site, drove his livery cab to the Brooklyn Bridge where he opened fire on a van occupied by Hassidic students, killing one of them: 16-year-old Ari Halberstam.

5. FEBRUARY 23, 1997: Abu Kamel, a Palestinian residing in Florida, selected the Empire State Building to carry out his intent of "annihilating" perceived enemies. He went to the observation deck on the 86th floor and shot seven people, including a Danish tourist who was killed. Kamel then turned the gun on himself and committed suicide.

6. JULY 31, 1997: the New York Police Department stopped a plot at the last minute to bomb the subway complex at Atlantic Avenue in Brooklyn. The bombers were assembling the devices when police officers entered their apartment and shot and wounded them before they could detonate the bombs.

7. SEPTEMBER 11, 2001: The World Trade Center was destroyed by al-Qaeda with the loss of more than 2,700 lives.

8. OCTOBER 2001: In the space of a week, employees and visitors at the New York Post, NBC, CBS, and ABC News in New York City fall victim to anthrax attacks. Later the same month, a New York City woman died of inhalation anthrax because of cross-contamination of mail she handled at work with that of the targeted media.

9. JUNE 2002: Security personnel from Iran's Mission to the United Nations were observed by NYPD videotaping landmarks and infrastructure. They were expelled from the United States by the State Department because of their suspicious activities.

10. LATE 2002 AND EARLY 2003: al-Qaeda operative Iyman Faris, on orders from his handlers overseas, twice examined the Brooklyn Bridge to evaluate the feasibility of destroying it.

11. NOVEMBER 2003: Two more security personnel assigned to Iran's Mission to the United Nations were caught by the NYPD video taping tracks and tunnel of the Number 7 subway line as it entered the tunnel under the East River. They returned to Iran soon after the incident.

12. APRIL 10, 2004: al-Qaeda operative Mohammad Babar was arrested by NYPD detectives and FBI agents in Queens, New York, for his role in a plot to bomb pubs, restaurants, and train stations in London.

13. JUNE 2004: Once again, two more security personnel from Iran's Mission to the United Nations were caught – this time by the FBI – videotaping sensitive locations in New York. Suspected of conducting reconnaissance of New York City landmarks and infrastructure, they were again expelled by the State Department.

14. JULY 2004: A laptop commuter of an al-Qaeda operative overseas is recovered. On it are detailed reconnaissance plans that show al-Qaeda operatives had been in New York City to plan an attack on the New York Stock Exchange, Citigroup headquarters in mid-town Manhattan, and the Prudential building across the river in Newark.

15. AUGUST 2004: A week before the Republican National Convention, two Islamic radicals from Brooklyn were arrested in a plot to bomb the Herald Square subway station. One pleaded guilty and cooperated with the investigation. The other was convicted in Federal court on May 24, 2006. He was found guilty on all four counts.

16. NOVEMBER 2005: Uzair Paracha, a Pakistani-born resident of New York City, was convicted of providing material support to al-Qaeda. While residing in New York, Paracha agreed to pose as an al-Qaeda operative, Majid Khan, in an attempt to disguise the fact that Khan had illegally left the U.S. for Pakistan. Paracha's father, who had met Osama Bin Laden, was part owner in a Manhattan garment district business. It was suspected that the ultimate goal was to use the Paracha business's shipping containers to smuggle weapons and explosives into New York City.

17. JUNE 2006: Syed Hashmi, a Queens resident active in the New York City chapter of a radical Islamic group known as al-Muhajiroun, was arrested in London where he was engaged in providing material support for al-Qaeda fighters in Afghanistan.

18. July 2006: A leak to the media revealed a sensitive investigation into an international terrorist plot to use suicide bombers to blow up New York City tunnels and flood lower Manhattan.

While the specific numbers are classified, it should be noted that the number of investigations ongoing at New York's Joint Terrorism Task Force significantly exceeds that of any other city in the nation.

In short, we believe that New York City continues to be al-Qaeda's number one target in the United States, if not the world.

In the view of the New York Police Department, the threat of terrorism is a global phenomenon that continually presents the possibility of manifesting, at any time, and with catastrophic consequences, in our city. Thus, while the NYPD has a great deal of knowledge of local extremist, radical, and militant individuals and groups, we are equally interested in indicators of terrorist activity elsewhere in the country and around the world. Our reason for this wide view is simple: as terrorists have demonstrated time

and again, the efficiency of modern transportation systems – commercial aviation, highways, trains and transit systems, etc. – permits our enemies to conceive, plan, and prepare attacks at far-flung locations, transferring the weapons or operatives to their final target at the last minute. The NYPD does not have the luxury of concerning itself only with our five boroughs, though we wish we did.

Globally, we have seen the central apparatus of al-Qaeda reduced to a fraction of its former self. We believe that the al-Qaeda leaders who remain at large have struggled, with little success, to resume offensive operational activity against the United States and our allies. While we cannot discount the possibility that "legacy" al-Qaeda will successfully mount an attack against the U.S. homeland or American interests abroad, Osama bin Laden and Ayman al-Zawahiri appear to have been transformed into leaders of an ideological movement rather than an operational organization.

More generally, because of continued offensive operations by the United States and its allies against some known international terrorist networks, as well as significant improvements in U.S. border security, the ability of any international or foreign terrorist organization to launch an attack into the United States from abroad appears to have diminished somewhat since late 2001. The NYPD takes no comfort in this analytic conclusion, however, because our baseline vulnerability was enormous.

We also believe that many of the most significant international trends that have bearing on the terrorist threat to New York City and the U.S. homeland are moving in a bad direction. In particular, we have observed a continued proliferation of extremist, often Salafist, militant ideology across the Muslim world. This ideology, with its literalist and generally intolerant worldview, as well as financial backing from a variety of different sources in the Persian Gulf, is a precursor to continued terrorism. Its spread shows no sign of abating; if anything, it is accelerating.

There is no single reason or simple explanation for the spread of extremist militant ideology across the Muslim world. The process has been underway for many years,

and undoubtedly much of the blame lies with the failures of the governments of nations with large Muslim populations to provide adequately for their people. Yet hostility toward U.S. foreign policy is clearly a significant motivating force among Muslim extremists and militants; there is ample evidence of this abroad as well as in New York City. Criticism of U.S. military action in Afghanistan and especially Iraq, coupled with American support for Israel, are consistently discussed among pockets of the Muslim community and serve as catalysts for radicalization. These political grievances have contributed to both the expression of extremist rhetoric and, more importantly, the development of a jihadist "soldier of fortune" mindset among some young male Muslims who want to "do something."

We have also seen evidence that this phenomenon has worsened as a result of recent events in Lebanon. In the last few months, we have begun to reconsider the threat of terrorist attacks against the homeland emanating out of the Shiite groups, such as Hezbollah, which have to date, for the most part, refrained from attacking the United States directly. We strongly suspect that these groups have the latent capacity to attack the United States directly and effectively. We are deeply concerned that, as result of events in the Middle East, they will elect to do so.

The most important trend that we have observed over the last several years is the rise of the "homegrown" threat, which has been widely commented on in the media.

Since September 11, 2001, most terrorist plots and attacks perpetrated worldwide have been conceived, planned, and executed by individuals who are part of the local populace and who have only limited, if any, transnational linkages to terrorist organizations abroad. Recent examples of "homegrown" terrorist plots and attacks abound: the recently disrupted terrorist plots in the United Kingdom and Canada, as well as the successful attacks against the London and Madrid subways, to name only four.

New York City is a microcosm of global demographic trends. It contains significant populations from over a dozen countries of terrorist concern. As militant extremism

proliferates throughout the world via the Internet, chatrooms, literature, videotapes, sermons, conferences, and traveling militant imams, its effects on foreign as well as domestic Islamic populations appears to be consistent. Despite the success of U.S. overseas efforts in degrading al-Qaeda as an organization, its powerful radical influence on the City's younger generation – especially among its sizeable Muslim community – continues to pose a serious threat from within.

We consider the fuel that ignites this inside threat – extremist militant ideology and influences – as the most critical challenge in addressing this inside threat in New York City. We are especially concerned with the radicalizing influence of the Internet, coupled with the potential role of its 2nd and 3rd generation citizens as the receptors of these influences and as the future radicalizing agents.

In addition, Islamic conversion and radicalization among the population in the prison system is a trend that may contribute to new threat emergence among the indigenous Muslim population. Within the prison system, inmates, seeking protection or prayer privileges, "convert" to Islam. Though most prisoners revert back to their original religion following their release from prison, a segment of the convert population continues their conversion process outside the prison. This process is aided and abetted by an imam/mosque network that guides recent parolees to particular mosques for employment, temporary housing and for some – international travel to the Middle East or South Asia for further indoctrination.

There is no question that many countries – the United Kingdom, for example – face a threat of "homeland" terrorism that is more acute than that faced by the United States. Again, the NYPD takes no comfort in this conclusion. The possibility of a "homegrown" terrorist attack against New York City or any other American city is real and is worsening with time as the radicalization process unfolds.

III. Recommendations

This is not the setting and, given my current position, I am not the person, to offer a comprehensive assessment of the federal government's efforts to secure the homeland or a comprehensive set of recommendations. Congress and the Federal Executive Branch have taken countless actions over the last five years that have significantly improved the security of the United States. It is not for me to catalog these achievements. At the request of the Committee, however, I will suggest the following areas in which the federal government could, by doing more or conducting itself differently, combat the threat of terrorism against the homeland more effectively.

Federal Counterterrorism. President George W. Bush and his principal officers have said repeatedly that the prevention of another attack against the homeland is the nation's top priority. The NYPD agrees completely. For five years, the country has been successful at this task. Our challenge – it is a daunting one – is to continue this success indefinitely.

Earlier in this statement, I outlined organizational reforms that the NYPD has undertaken to better protect New York City and to improve our ability to thwart terrorist plots before they manifest as attacks. In parallel, the U.S. government has enlarged and reformed virtually all of its federal agencies with counterterrorism responsibilities. Much progress has been made, but this extremely important process is by no means over. I will confine my comments on this process to the NYPD's most important federal partner in the field of counterterrorism, the Federal Bureau of Investigation.

The NYPD has an excellent partnership with the FBI's field office in New York. As I mentioned before, over 100 NYPD detectives are assigned full-time to the Joint Terrorism Task Force in New York City. The JTTF permits the awesome power of the federal government's national intelligence capabilities to be brought to bear against any particular terrorism case, subject, of course, to the Attorney General's guidelines, the

customary bureaucratic procedures of the FBI and the Department of Justice, and the cooperation and effectiveness of the intelligence collectors.

The NYPD agrees with the President, the Attorney General, the FBI Director, and the 9/11 Commission on the vital need to transform the Bureau into an agency with a robust, effective domestic intelligence capacity and an absolute priority on prevention of terrorist attacks. Reforming a proud and powerful organization like the FBI is always a difficult task. We fully support FBI Director Robert Mueller's plans for achieving his ambitious goals. We believe that it is vitally important that the implementation of Director Mueller's reform agenda not lose momentum as the memory of September 11, 2001, recedes.

The rise in the "homegrown" terrorist threat underscores the importance of an effective domestic counterterrorism and intelligence program. It is no secret that the preponderance of the federal government's unilateral intelligence collection and counterterrorism activities, as well as its liaison relationships and joint operations with partners in the war on terror, are directed against terrorist operatives and networks abroad. These intelligence and counterterrorism activities abroad are tremendously useful in combating transnational terrorist threats: when a terrorist group seeks to deploy into the United States from abroad, as the 9/11 hijackers did, a lead generated abroad can quickly lead to the individuals already in, or trying to enter, the homeland.

But "homegrown" terrorists, by definition, have only limited, if any, linkages across national boundaries. Thus, compared to transnational terrorism, there are relatively fewer benefits to be gained in combating "homegrown" terrorism from the federal government's vast intelligence and counterterrorism program abroad. While no comprehensive accounting of the country's expenditure and investment on domestic as opposed to international counterterrorism has ever been conducted, it is clear that the domestic element is but a small fraction of the international element.

The implications are obvious: the country is under-investing in the sort of capabilities most needed to combat the most dynamic element in the spectrum of terrorist threats – the "homegrown" element – to the homeland. In combating "homegrown" threats, the burden shifts instead almost entirely to local law enforcement. A "homegrown" threat, like the terrorist plot against the Herald Square subway station disrupted by the NYPD in August 2004, presents few obvious inherent indicators and the few signatures are subtle and embedded within the daily activities of a vast civilian population. Such threats are most likely to be detected by dedicated investigators with both intimate knowledge of the population in question and mastery of human intelligence tradecraft who are backed by the full power and resources of a major law enforcement agency.

This is one of the reasons why the NYPD has decided to augment its joint counterterrorism investigative work with the FBI with an organizationally distinct intelligence program operating under separate legal authorities. Put differently, in the NYPD's view, a reformed FBI and an aggressive, genuinely *joint* Joint Terrorism Task Force are necessary – indeed, are vital – but are not sufficient to combat the threat we face. So far as I am aware, the only such domestic intelligence program in the United States today is the New York Police Department's.

An important question for the Congress and the Administration is whether some additional domestic intelligence and counterterrorism capacity is required in the rest of the country.

Information Sharing. Most federal officials and outside experts recognize the need to share terrorism-related information with state and local law enforcement agencies. The reason is obvious. The right piece of intelligence, in the right hands, can lead to the identification of a potential threat and, possibly, to the prevention of a terrorist attack. The country learned this lesson the hard way in the aftermath of the attacks of September 11, 2001, when then-Director of Central Intelligence George Tenet acknowledged the CIA's failure to inform the FBI, the State Department, and local agencies that two known al-Qaeda operatives – Khalid al-Mihdhar and Nawaf al-Hazmi

– had entered the United States. Hopefully, this is the last time our country will learn this lesson.

Given my personal experience with this issue while serving on the White House staff, I know the enormous difficulty of building an effective interagency and intergovernmental information-sharing system. It is vital, however, that the federal government continue the effort.

From my new vantage point within the New York Police Department, my observation is that the federal government, while well-intentioned, has no overarching vision for terrorism-related information sharing with state and local agencies and no clear federal direction or leadership. Part of the problem was made clear by the Government Accountability Office in its March 2006 report, which identified 56 different sensitive but unclassified designations that federal agencies use "to protect information that they deem critical to their missions." At least three Cabinet-level officers – the Secretary of Homeland Security, the Attorney General, and the Director of National Intelligence – have substantial oversight responsibility for the federal government's information-sharing system; none of them appears truly engaged by the topic. The only established information-sharing mechanism with real coherence and consistent value is the sharing of usually case-specific, classified information with the Joint Terrorism Task Force; this mechanism works reasonably well for what it is, but even it has significant limitations. From the NYPD's perspective, the utility of the Department of Homeland Security's information-sharing initiatives is severely limited by DHS's apparent inability to treat various state and local agencies differently according to their role, their sophistication, their potential contribution to the national mission of combating terrorism, and their size and power. Consequently, NYPD's collaboration with other members of the Intelligence Community and with foreign law enforcement and intelligence agencies is substantially more valuable than is our collaboration with DHS.

In information sharing, the quest for perfection is a fool's errand. So is the quest for absolute control. The right model of *intergovernmental* information sharing is precisely

the same as the right model of *interagency* information sharing – namely, a massively interconnected network. State and local agencies with major investments in intelligence collection and highly sophisticated analytic capabilities should be able to access existing federal classified information networks without prejudice so long as they obey the same rules and regulations as all other participants in the network. A pipeline, in which one or a few agencies seek to tightly control the flow of classified or sensitive information to state and local agencies, is exactly the wrong conceptual model for intergovernmental information sharing; any effort to impose such a model on agencies such as the NYPD would be a major step backward with extremely problematic consequences.

The Terrorist Watchlist. There is one particularly important form of information sharing that deserves urgent attention and should be utilized much more aggressively. As a result of Homeland Security Presidential Directive 6 and the first-rate work of retiring director Donna Bucella, the Terrorist Screening Center (TSC) has developed an integrated terrorist watchlist for the entire United States, supported by a 24/7 operational support center. This institutionalization of an integrated watchlist is one of the many relatively small, but important, successes that generally go unnoticed.

The Terrorist Screening Center has been a great success. My concern is that the capability it provides is not being used extensively enough by the U.S. government, state and local agencies, or the private sector. Aside from a few well-established screening procedures, such as visa applications, border entries, and criminal records checks, the country is missing countless perfectly lawful opportunities to screen lists of names against the watchlist. The federal government needs to do a much better job of promoting the widespread utilization of watchlist screening. One aspect of this effort should be TSC's incorporation of technology that will permit a "blind" (or "anonymized") query against the watchlist – that is, a query that will not reveal the personal information of the individual being checked against the list to any law enforcement or intelligence agency unless there is a positive "hit" against the list.

Among the many venues in which the federal government could but is not routinely screening individuals against the terrorist watchlist, the most egregious is undoubtedly domestic aviation. (Passenger manifests of inbound international flights are checked against the watchlist, but currently only 15 minutes after their flights take off; the NYPD supports the Department of Homeland Security's recent proposal to require watchlist checks against the passenger manifests of inbound international flights prior to their takeoff.) Despite the existence of the terrorist watchlist, despite unambiguous regulatory authority, despite repeated terrorist plots and attacks against aviation, and despite a statutory requirement to do so, the Transportation Security Administration still has not deployed a system that will permit the real-time, automated checking of passenger and crew names against the terrorist watchlist for domestic flights or outbound international flights.

Critical Infrastructure Protection. As one of the original architects of the Department of Homeland Security, I say with some sadness that there is no area of the Department's work that disappointments me more than critical infrastructure protection. The problem was rather embarrassingly illustrated by the DHS Inspector General's report that DHS had a database of our nation's vulnerable critical infrastructure, key resources, and national assets that included sites such as Old MacDonald's Petting Zoo in Alabama, a bean festival in Georgia, and the world's largest tin foil ball in Ohio.[1]

The New York Police Department has assessed countless potential terrorist targets in the City, and we monitor the construction or renovation of new potential targets. We have ranked them in terms of the danger they present using defensible analytic criteria. We maintain and carefully guard this list. We maintain a file on each of those potential targets that we assess to present the most serious danger to New York's residents, commuters, and visitors and to New York's economy. And most importantly, we take action to reduce the inherent vulnerability and danger of these top-priority targets.

---

1. http://www.dhs.gov/interweb/assetlibrary/OIG_06-40_Jun06.pdf

The precise combination of actions we take depends on the particularity of each potential target. In some cases, we may emplace or require the emplacement of bollards on the curb. In others, we may temporarily close a street to vehicle traffic, or put in place a vehicle screening check point. In others, we may engage with the owners or real estate developers to convey our sense of the appropriate design basis threat for a new building, and to ensure that these requirements are followed through construction and operation of the building. In other cases, we may deploy a radio car – or perhaps even a harbor launch – with armed officers to an access point to a particularly critical vulnerability. In still others, we might install or require the installation of protective fencing around a particular vulnerability, such as bridge cabling. These measures, and countless other steps like them, constitute critical infrastructure protection. DHS does hardly any of this and provides only marginal assistance to us as we do it.

In addition to more generous grant support, if the federal government wanted to provide more consequential assistance to the state and local agencies that are actually attempting to protect critical infrastructure, it could do two things.

First, the federal government could recommend a design basis threat and blast performance standard for all major, newly constructed buildings for inclusion in state and local building codes. The Department of State, the Department of Defense, and the General Services Administration currently set such standards for federal facilities. The country as a whole, however, has no such standards though we note that the National Institute of Standards and Technology has recently released a draft set of new construction design standards for comment. The result is that, with few exceptions, major new buildings are being built all across America with almost no regard for their ability to withstand the effects of a curb-side VBIED. Cities such as New York are forced to grapple with this issue on an ad hoc basis, without any consistent national framework.

Second, the federal government could intervene in the insurance market to promote private-sector insurance against terrorism risk. The percentage of commercial real

estate that is insured against terrorism risk has fallen dramatically over the past five years. This development is worrying for a number of reasons, the most important of which is that it reduces an important, market-based incentive for private property owners to build and maintain their facilities to a higher security standard. The disappearance of commercial insurance against terrorism risk has been caused by a number of different factors: most important is that the primary insurers now generally exclude terrorism risk from their standard commercial policies, in some cases not insuring against terrorism risk at all, while in others, selling separate—and quite expensive—terrorism-risk insurance policies, which policyholders generally elect not to take. There is no mandate or expectation that commercial policy writers will insure against terrorism risk.

The market will not address this problem and federal action to date has been inadequate. The Terrorism Risk Insurance Act (TRIA), which was scheduled to sunset in 2005 but extended by Congress to 2007, merely backstopped the reinsurance firms that underwrite primary insurance companies. TRIA's backstopping of the reinsurance market may be necessary but is clearly insufficient for security purposes. To reverse this trend away from terrorism risk insurance across the nation, the federal government should consider adopting, as national policy and law, the mandatory inclusion of terrorism risk in all commercial insurance policies nationwide, without regard to location.

Chemical Security. This committee knows my views on chemical facility security and the need for new legislation from my April 2005 testimony. Poorly guarded toxic industrial chemicals represent the most severe and widespread mass casualty vulnerability in America today. My view of this matter has not changed since I joined the New York Police Department.

Since 9/11, there has been no meaningful reduction in the inherent vulnerability of toxic industrial chemicals in facilities or in transit to a terrorist attack. The Executive Branch has elected not to use its existing statutory authority to improve the security of

chemicals in transit, and lacks the statutory authority to require security improvements at chemical facilities.

I know this committee agrees with me that Congress should enact, and the President should sign, a law which provides the Secretary of Homeland Security the authority to impose risk-based security regulations on chemical plants. With only a few legislative days remaining before adjournment, it now appears certain that the 109th Congress will send no such bill to the President's desk. It is patently obvious that the issue of chemical security is a priority for neither the President nor the Congressional leadership. This is a great disappointment. One can only hope that the 110th Congress will take the matter more seriously.

Ammonium Nitrate Security. Another area in which Congress has failed to act, and in which the Executive Branch has shown no leadership, is the regulation of ammonium nitrate fertilizer. It has become commonplace to ask why, five years after September 11, certain security enhancements have not been implemented. In this case, the question is "Why has nothing been done about ammonium nitrate more than ten years after the Oklahoma City bombing?"

In April 1995, Timothy McVeigh and Terry Nichols destroyed the Alfred P. Murrah Federal Building in Oklahoma City with a 4,000 pound main explosive charge that consisted of ammonium nitrate fertilizer, nitromethane (racing fuel), and fuel oil. McVeigh and Nichols procured the ingredients lawfully and easily. They mixed the ingredients in 55 gallon plastic drums and measured the quantities with a five gallon bucket and bathroom scale.

The commercial explosive ammonium nitrate and fuel oil, also known as ANFO, is the cheapest and most widely used explosive in the United States. ANFO is subject to tight federal regulation under USC Title 18. The problem is that the ingredients needed to make this explosive may still be purchased *separately*, with ease and with no significant security checks, just as McVeigh and Nichols did in 1995.

To demonstrate this, in September 2004, the NYPD Counterterrorism Division conducted a red cell operation in an effort to acquire ammonium nitrate fertilizer and other materials to construct a VBIED. On two occasions, NYPD investigators purchased approximately 1,000 pounds of ammonium nitrate fertilizer at retail outlets within and outside New York State. The operation proved the ease with which the fertilizer can be legally obtained and used as part of an explosive device.

As in the case of chemical security legislation, and despite the efforts of this committee and the House Committee on Homeland Security, it has now become virtually certain that the 109th Congress will fail to send to the President's desk legislation that would impose strict regulation on the sale and purchase of ammonium nitrate fertilizer. As a result, it is today, and will remain for the foreseeable future, as easy for a terrorist to build a truck bomb as it was for McVeigh and Nichols to do so more than ten years ago.

Port Security. Port security has received an enormous amount of attention since 9/11. According to a recent estimate, funding for port security has increased 700% since September 11, 2001. DHS is reported to have spent $1.6 billion on port security in FY2006.

However, the threat that seems to dominate discussion among federal policymakers and the media is the theoretical possibility that a terrorist organization will use the cargo shipping system to deliver a dangerous weapon into the United States. Our view is that while this threat cannot be discarded entirely, its significance has been greatly exaggerated. In our view, the most significant port security threat is an improvised explosive device borne by a small boat – that is, the precise method used by al-Qaeda in its successful attack on the USS Cole in Yemen in October, 2000. With a few exceptions, the federal government has done very little to help protect America's waterways and congested ports against this threat, generally leaving state and local agencies to their own devices. DHS's port security grants are overwhelmingly biased toward cargo and container security; these funds should be redirected to support relevant security operations on the water.

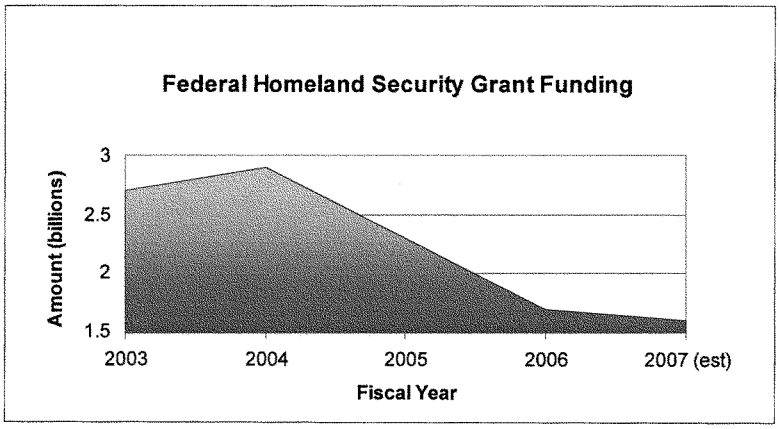
"Securing the Cities" Against Radiological and Nuclear Threats. The NYPD was intrigued when, on July 14, 2006, the Secretary of Homeland Security announced the "Securing the Cities" initiative, starting with New York City. We are currently working with the Domestic Nuclear Detection Office (DNDO) to explore the technical and operational viability of an intelligent, integrated metropolitan sensor network that goes beyond radiation pagers and a few mobile sensors. The NYPD shares the federal government's concern with the radiological/nuclear threat, and are hopeful that a comprehensive defensive system proves technically and operationally viable.

It will be vital, however, for the Administration to request and Congress to appropriate funds specifically to support the development, deployment, and operation of the Securing the Cities initiative. If states and cities are expected to fund these efforts through the use of existing DHS grant programs, the initiative is certain to fail.

Mass Transit Security. The NYPD is profoundly concerned by the threat of attacks on mass transit systems. The New York City transit system is the largest in the nation with 840 miles of track, 468 stations, and 4.5 million passengers per day. New York City has only 35 fewer stations than all of the other subway stations in the country combined.

The responsibility for transit security ultimately lies at the local level but more financial support is needed. There are 2,635 NYPD transit officers assigned to police this system. In addition to their traditional crime fighting role, these officers play a central part in supporting counterterrorism and terrorism interdiction operations in a high threat environment. These officers, for example, are primarily responsible for implementing the Department's important Counterterrorism Container Inspection program. The very nature of the transit system, with its confined spaces, heavy mechanical equipment, and dense ridership, demands that these officers be prepared to act decisively and efficiently with minimal supervision under the most extreme and dangerous conditions. This commitment at the local level to protect the New York City transit system against an enemy of the United States deserves significant and continued support from the federal government.

Since 9/11, the investment in mass transit security as opposed to aviation security is widely disproportionate. Billions of dollars have been spent since 9/11 on aviation security; only a small fraction of the money spent since then has been devoted to mass transit security. According to the findings contained in the Public Transportation Security Act of 2004, the federal government has invested $9.16 per passenger in aviation security but only 0.6¢ for each transit rider. The federal government must do a better job of investing in transit security. It may be possible for the federal government to take the perspective that an attack on mass transit is inevitable – but as officials in NYC, we do not have that luxury.



Federal Homeland Security Grant Program. From my previous work in the White House, I know that the allocation of grants is a thankless job. Nevertheless, the federal government can do a much better job than it is doing now. I believed this before I joined NYPD and believe so even more today.

I will limit my comments on the federal homeland security grant program to six main points.

1. The size of the overall federal homeland security grant budget, as shown in Table 1, has fallen to an indefensibly low level. In the President's FY2002 Budget, the first released after the terrorist acts of September 11, 2001, the Administration requested and Congress ultimately appropriated roughly $3.5 billion in new "first responder" grants. In the coming days, the House-Senate conference is expected to recommend an appropriation of roughly $1.6 billion in total homeland security grant funding, a drop of $1.9 billion from the first post-9/11 budget. By contrast, according to the Congressional Research Service, the U.S. government has spent approximately $10 billion per month in FY2006 to support military operations in Iraq and Afghanistan. Given the rise in the "homegrown" terrorist threat described earlier in my testimony, and the essential role of state and local agencies in combating this threat, this vast disparity in federal outlays simply cannot be justified.

2. As the 9/11 Commission recommended, all of the funds appropriated by Congress for homeland security grants should be distributed solely on the basis of risk. The former 9/11 Commissioners, in assessing the federal government's implementation of its recommendations, gave the Congress a grade of "F" on this issue. Politically derived formulas embodied in statute should play no role in the disbursement of funds needed to protect the homeland from terrorist attack.

3. To the extent that Congress nonetheless requires the distribution of homeland security grants to the states on the basis of formulas embodied in statute, the Department of Homeland Security should require that governors distribute these funds on the basis of risk. Furthermore, these intra-state risk-based allocations should in no way prejudice a city's allocation of additional DHS risk-based grants.

4. DHS should reconsider and revise its mechanism for distributing discretionary grant funds in FY2007. The mechanism used by DHS in FY2006 was incomprehensible, incoherent, and an embarrassment to the federal government. In particular, any methodology which determines that New York City has only four financial institutions and no "national monuments and icons" should be scrapped. DHS's use of so-called "peer review panels," managed by Beltway contractors, to evaluate the effectiveness of NYPD's intelligence and counterterrorism programs is equally preposterous. DHS and the peer review panels apparently view counterterrorism operational investment as a purely local matter, for which the federal government is not responsible, since it is a local function performed at local expense by local personnel already in place. We see our ongoing initiatives, like Operation Atlas, as a necessary component of our strategy to prevent terrorist planning and attack, worthy of federal investment in the ongoing personnel costs required to sustain it.

5. Currently, all DHS grant programs are biased toward the expenditure of funds for equipment, external consulting, and consequence management at the expense of manpower, current operations, and counterterrorism and intelligence activities designed to prevent attacks before they occur. This bias makes no sense given the evolving terrorist threat facing the U.S. homeland and the operational requirements to counter it. Time and time again, well-trained law enforcement personnel have thwarted potential terrorist attacks. It is fair to say that the most effective tool in our counterterrorism arsenal is manpower. In a recent study undertaken by the NYPD of more than 20 terrorist plots that were successfully thwarted in the last decade, NYPD analysts found that technology was not integral in the prevention of any of them.

6. The Congress would be ill-advised to condition a city's receipt of homeland security grant funds upon that city's policies regarding contacts between city employees and the Bureau of Immigration and Customs Enforcement relating to an individual's immigration status. The homeland security appropriations bill

passed by the House would do just this. We can all agree that immigration policy is a controversial and divisive subject in American society. It would be foolish to hold hostage a city's ability to protect itself from terrorist attack over ongoing political disagreements over immigration.

The country needs human intelligence to disrupt terrorist planning, like the plot to bomb the Herald Square subway station and the conspiracy recently revealed to attack multiple targets in Ontario, Canada. We need to dedicate officers to specific counterterrorism and homeland security missions, around the clock, on overtime as needed, to protect prime targets. We need to train them throughout their careers to contend with emerging threats and to use the equipment that federal funds may purchase. It appears that New York City is being disadvantaged because we are ahead of the curve, and that our funding needs are different from those of many other jurisdictions precisely because we have attended to so many of these needs ourselves, for so long. We need the federal government to step up and adequately share the burden of these ongoing costs to defend vital national assets in New York.

IV. Conclusion

Thank you once again for affording me, as a representative of the New York Police Department, the opportunity to appear before you today. I would be happy to answer any of your questions.

Statement of Steven N. Simon
Senate Committee on Homeland Security and Governmental Affairs

"Priorities for Homeland Security"

Thank you for the opportunity to address the committee on this vital topic.

Just as a preamble, my remarks do not reflect the views of the Council on Foreign Relations, which does not have a corporate position on these matters.

My understanding of the Committee's objectives in holding this hearing is that witnesses should focus on the future and address themselves to issues that might help both Congress and the Executive branch set homeland security priorities. The Committee it seems to me is doing the right thing. Our vulnerability at home to terrorist assault, as well as to natural disasters, is essentially infinite. The fact is that not everything can be protected. Judicious decisions about what to protect given our wholesale and inevitable exposure to attack by clever and disciplined terrorists are essential.

What follows are my personal reflections on this vexing problem. Given the myriad threats to our infrastructure – critical and otherwise – and to the lives of our fellow citizens, other analysts will legitimately come to different conclusions about the best way to focus our collective efforts and especially those of the agencies under the jurisdiction of this committee, and of departments and agencies with which DHS must interact continuously and cooperatively in order to fulfill its daunting mandate.

I will concentrate on three issues: first, the importance of cities as terrorist havens and terrorist targets; second, the continuing significance to many jihadists of weapons of mass destruction (WMD); and third, the need to preserve the good will and sense of belonging of America's Muslim communities as a matter of national security, beyond the intrinsic virtues of a cohesive, considerate society in which citizens of all creeds can feel at home.

Urban Warfare

The jihad that has evolved since September 11th has become a war of cities. The transition from caves to condos, as one observer described this evolution, is impressive. Although the relatively remote, rural bases that incubated the jihad had strong advantages, especially given the centrality of social networks to the early jihad, municipalities have their own attractions. They offer anonymity, but also community, both of which can confer a kind of cover. Urban neighborhoods, with their numberless apartments, coffee-houses, mosques and Islamic centers, provide the setting for recruitment, clandestine meetings, preparation of weapons and other activities that form the terrorist enterprise. Moreover, the majority of urban areas in which jihadists have established a presence are not targets for air strikes, Hellfire missiles, or submarine-launched cruise missiles. Think of Muhammad Atta's Hamburg, or the Leeds of Muhammad Siddique Khan, orchestrator of the 7/7 bombings of the London underground

and bus systems. Post-bin Laden jihadists are not the first militants to avail themselves of these tactical conveniences. The radical campaign in Egypt that began in mid-1970s was spawned in Cairo, one of the world's largest cities. And of course non-Muslim terrorist organizations, such as the Provisional Irish Republican Army (IRA), have long thrived in urban areas. It could be said that having adapted to city life, the jihad has really come into its own.

Qualities that favor the jihadists' defensive requirements do not tell the whole story. The other side is that cities are where their targets – both symbolic and of flesh-and-blood – are to be found in abundance and proximity. There are many aspects of Islamist militancy that are quintessentially modern. The transformation of cities into fields of jihad is a classic example of the movement's modernity. It is part and parcel of the post-World War II process of urbanization that swept the Middle East, North Africa and Pakistan. Large-scale migration of Muslims to Europe represents perhaps the last phase of this urbanizing process. In these cities, Muslims radicalized by a potent combination of powerful imagery in the media, socio-economic exclusion, and a set of simple, but internally consistent religious and ideological concepts, have ample targets for their hunger for retribution and duty – from their perspective – of self-defense. One of the striking features of contemporary Muslim public opinion to emerge from recent Pew polls is the degree to which Muslims in far-flung, diverse places have come to see themselves as having "more in common nowadays." This attitude can be seen at work in the United Kingdom, Spain, Germany, The Netherlands and Denmark. Events far removed geographically from these countries, especially developments in Iraq, have mobilized youth in each of their capitals.

New York has already shown itself to be a crucial target for jihadists. This great city was construed by al-Qaeda to be the beating heart of America's economy, which bin Laden believed he could cripple; the symbol of American arrogance as embodied by the "looming towers" of the World Trade Center; and the seat of Jewish power, which jihadists believe accounts for the global subordination of Muslim interests to America and Israel. It is also a teeming city, whose large and densely packed population promised the most efficient path to a successful mass attack that –from a jihadist viewpoint -- might begin to even the score with the United States. There is no reason to think that this conviction has weakened. Furthermore, New York City proffers the same advantages to the attacker as do all large cities.

The array of targeting opportunities in New York is wide. Although we can be perversely certain that the attack, when it comes, will be the one we least expected, some preliminary judgments are possible. Mass transportation, which the jihadists have attacked elsewhere with some success, the financial district or banks, symbols of authority, and perhaps schools, given al Qaeda's insistence on the need to avenge the tens of thousands of Muslim children it believes were deliberately killed by the U.S., either directly or through Israeli action thought to be sponsored by Washington. Car or truck bombs -- the icon of urban violence in Iraq and used effectively before then in Lebanon and Argentina by Hezbollah and elsewhere by others including the IRA, the Basque separatist group ETA and the Baader-Meinhof gang -- should also be expected at some

point. Similarly, we might expect Palestinian style backpack bombs carried into restaurants or other public places by solitary suicidal attackers.

The implications of this analysis are, first, that community policing and extensive video surveillance probably need to be stepped up. In this kind of urban warfare, intelligence is acquired best by those who are most familiar with the terrain: police officers walking their beat. On the front line, they get to know their neighborhoods, the residents and the shopkeepers, form and cultivate relationships with local citizens, and develop a sense of the natural order of things and therefore of signs that something is out of the ordinary or warrants investigation. The pivotal role of local law enforcement is reinforced by the incapacity of federal authorities to gather information skillfully, discretely, effectively, and without alienating potential sources of intelligence. The FBI, in particular, presently lacks the numbers, skills, knowledge base and orientation to contribute.

This does not mean however that local law enforcement can or should operate in a vacuum, especially in light of connections that have been disclosed between the self-starter groups in the U.K. and al-Qaeda figures in Pakistan. On the contrary, local police need an umbilical connection to national intelligence agencies in order to connect the dots they're collecting on the ground. It is worth noting that the success of the UK counterterrorism effort in Northern Ireland was largely due the tight linkages between the local police, national police, and Britain's domestic intelligence agency that were forged early in the conflict.

Yet information sharing, which all parties claim to be essential, has not advanced significantly. In part this seems to be due to a lack of leadership, and in part to a slow pace of work that seems incommensurate with the urgency of the threat. Thus, issuance of U.S. government sponsored clearances for local police officers, the necessary first step toward sharing intelligence information, has lagged. Even the New York Police Department (NYPD), which has built a very aggressive intelligence collection program and uncommonly close ties to Washington intelligence agencies, has only about 350 cleared officers, or less than one per cent of the force. Many of these patrolmen and detectives have clearances via their status as military reservists rather than as police officers. Countrywide, cleared personnel are usually the handful of detailees to the local Joint Terrorism Task Force. The circle clearly needs to widen.

The other dimension to this issue is the apparent substitution of quantity for quality as Washington's criterion for information sharing with local law enforcement. This puts municipal authorities in the worst of both worlds. The information does not help them do their jobs better, while the sheer volume of unhelpful information can make it harder to manage their responsibilities.

The bigger question, however, is where these police officers will come from, at a time when State, local and federal budgets are under severe pressure. In the upcoming federal budget cycle the COPS program is again under pressure to be cut. This program has put more than 100,000 new police officers on the street over the last decade. Instead of

eliminating this program it should be revamped to create the local intelligence capacity cities need.

WMD

Amid growing concerns about the vulnerability of ground transportation, civil aviation, financial institutions and landmarks to large bombs, one should not lose sight of the chemical, biological, radiological and nuclear threats. As many experts have usefully pointed out, jihadists, like other terrorists, prefer tried-and-true methods and shy away from technical innovation. This is certainly true as a general proposition, despite important exceptions, from the first use of dynamite by anarchists early in the 20th century to the experimentation with stabilized liquid explosives by Ramzi Ahmed Yousef in 1995.

Yet intramural jihadist tactical and strategic discussions frequently refer to the use of one or another form of weapon of mass destruction. Not every contributor to this debate defines the utility of these weapons in the same way. For some jihadists, WMDs are the golden key to a reversal of fortune, for which the Muslim world allegedly yearns. Others see these weapons in less apocalyptic terms and more as tools for "worldly war." For these jihadists, unconventional weapons are the indispensable instruments of the weaker party in an asymmetric struggle. Whether such a weapon is used in the belief that it will decisively settle the argument between Muslims and their chief enemy, or in pursuit of tactical effects meant to deter the enemy or deny him specific options, a toxic or radiological release or detonation of a nuclear weapon would have dramatic consequences.

The social and economic effects would obviously be proportional to the damage, but the baseline for these effects would be high. Thus, most experts believe that if such a weapon is used it is unlikely to cause mass casualties. Nevertheless, even an attack that took relatively few lives would have an emotional and psychological impact that could tear the fabric of our society and undermine the social contract between government and society. It would also have sizable, perhaps open-ended economic costs, especially if the attacks were repeated or authorities could not assure citizens that the attackers had all been captured or killed. The implication here is twofold. First, Washington must make consequence management a priority. This means not only allocating appropriated funds, but also establishing a high, federally defined performance standard that cities would have to meet reasonably swiftly. The reason for this emphasis on consequence management is simply that a well-planned attack will be difficult to prevent without an uncommon dose of good luck. This being the case, the surest way to stave off the worst emotional, political and economic damage is to show not only the victimized community, but also the American public that the effects of the attack are being handled with confidence and competence by local and federal authorities working quickly and smoothly – and in lockstep.

Efforts to do this have been broached repeatedly, ever since the second Nunn-Lugar bill was signed into law in 1996. Some of these initiatives failed because the government

was not structured in a way that yielded a lead agency that could or would be held responsible for this important job. Now that we have a Department of Homeland Security, this impediment has been swept away. It is now time to systematize consequence management where it matters most, which is in large American cities.

The other implication is that Washington and local leaders must begin soon to educate the public about the kind of CBRN attacks that are likely to occur. The purpose is not to scare people. Rather, it is to ensure that Americans understand that for the foreseeable future, a CBRN attack will not necessarily equate to instant annihilation, that it is likely to kill or wound relatively small numbers, and that the federal government and local authorities are prepared for such an eventuality. This is easier said than done, owing to the non-trivial risk that terrorists acquire a weapon capable of a catastrophic nuclear yield. An educational initiative would have to acknowledge this possibility, even as it strove to counter the effect of the Katrina aftermath on public confidence in the competence of their government.

As part of this effort, dedicated broadcasting channels should be set up so that authorities can communicate with the public throughout a crisis and so that the public knows exactly how to "tune-in" to this source of information and guidance. Given the plethora of electronic media and the scarcity of bandwidth, operationalizing this recommendation will not be easy. In a crisis, however, we will wish we had it available.

It goes without saying that the trans-attack and post-attack message must be fully coordinated among federal state and local agencies. It will be just as vital for all these players to have decided beforehand who will be empowered to speak publicly and about what. In the absence of such discipline, the public will be awash in contradictory and inconsistent statements and quickly conclude that no one is in charge. This perception will fuel the panic and desperation latent in what will be a terrifying and unprecedented situation.

Muslim-Americans

The 9/11 disaster showed that skilled, self-possessed and highly determined attackers could do tremendous damage to the homeland without having to rely on a support network within the United States. Halting and uneven progress on border security, especially at airports, has reduced the probability of this sort of attack by injecting uncertainty into terrorist calculations of their chances of getting in. Deterrence at that level does seem to work.

This type of attack, however, is not the adversary's sole option. Other approaches do require infrastructure, in the shape of cells that may or may not be linked to outside networks. A glance toward Western Europe, where this phenomenon seems to be well established, raises questions about circumstances here at home.

The conventional wisdom is that Europe's Muslim's discontent is a result of failed immigration policies that could not affect America's prosperous, happy Muslims, who

have benefited from the welcoming embrace of our "melting pot" nation. This view may not reflect reality, even if it once did. Recent research shows that "the real story of American Muslims is one of accelerating alienation," which could produce a "rejectionist generation."

Muslims are increasingly choosing not to assimilate into American society, finding solace in their religious identity instead. Muslim students' associations on college campuses are growing rapidly as havens for Muslims who prefer not to socialize with non-Muslims, and Muslims are building Islamic schools as alternatives to a public school system perceived as inhospitable. To thwart media bias, Muslims are developing their own radio programs and publications. These initiatives may resemble those taken by other religious and ethnic groups in the United States since the nineteenth century to promote acceptance and assimilation. But the Muslims' situation differs in that many perceive their nation's foreign and domestic policy agenda as a campaign against their faith.

The domestic aftermath of the 9/11 attacks implied that a low religious profile was better for their health, that they couldn't take their civil rights for granted, and that their interests depended on the absence of serious future attacks within the United States. Iraq further dimmed America's promise to its Muslims. The U.S. Muslim community is deeply skeptical about U.S. democracy promotion, which many think are undercut by lack of due process at home and support for authoritarian rulers abroad. In particular, Muslims vocally decry what they see as the biased implementation of the USA PATRIOT Act and the absence of official American sympathy for the victimization of Muslims worldwide, especially Palestinians.

The evolving attitudes of non-Muslim Americans towards their Muslim compatriots are likely to spur alienation. According to a 2006 Gallup poll, a third of Americans admire "nothing" about the Muslim world. Nearly half of all Americans believe the U.S. government should restrict the civil liberties of Muslim Americans. Since September 11, they have faced increasing racism, employment and housing discrimination, and vandalism. The Justice Department has undertaken high-profile prosecutions based on meager evidence, flawed procedure or misidentification. Media coverage dwelling on the violence associated with radical Islam, and ignoring the respectable lifestyles of most American Muslims, along with rhetoric of some on the Christian Right casting the war on terrorism as a clash of religions, contributes to the public's misunderstanding of Islam.

To be sure, Muslims in the United States have shown no sign of violent protest, and American Muslims' relative prosperity may function as a brake on radicalization. Yet U.S. Muslims' post-9/11 insularity suggests that some, like many European Muslims, may seek psychological sanctuary in the *umma* – that is, the notional global community of Muslims. And the *umma* is where Osama bin Laden's brand of militancy has maximum traction.

The U.S. government also has not manifested trust in the nation's Muslims. While the pool of Muslims available for official duty may not be large, the federal government has made no serious efforts to recruit Muslims for confirmable policy positions. Meanwhile,

mutual distrust has burgeoned. The U.S. administration should consult American Muslims directly and earnestly on foreign-policy issues, as is it has customarily done with other politically important minority constituencies – e.g., American Jews with respect to Israel, Irish-Americans on Northern Ireland, and Greek-Americans as to Turkey and Cyprus. The difference here is that the electoral leverage of American Muslims is relatively weak. But their potential vulnerability to an incendiary ideology of confrontation that is being disseminated transnationally should override the normal course of domestic politics. Fear of being punished at the polls should not be the only incentive to be more attentive to Muslim concerns and anxieties.

Finally, the Madrid and London bombings only confirm that governments need to understand the campaign against transnational Islamist terrorism as an internal security problem to a much greater extent than they have so far. The current approach, however, has been simply to enforce a zero-tolerance immigration policy with respect to the Muslim community. This dispensation has the doubly perverse quality of being both ineffective in counter-terrorism terms and alienating with respect to Muslim Americans. Domestic law enforcement's ranks should also include more Muslims, both to improve the FBI's understanding of and links with Muslim communities and to give Muslims a sense of ownership of America's security challenges. American Muslims do not remotely pose the domestic threat that European Muslims do. To ensure it stays that way, they need to be embraced – not spurned.

I put this issue before the committee for lack of a better place. The challenge outlined here requires leadership and a program. Yet given the way our government is structured, there is no obvious lead agency, or special assistant to the President on the National Security Council or Homeland Security Council, to formulate a program or provide the leadership. We are not the first to face this conundrum. Several years ago, in the wake of a Whitehall study showing upwards of 10,000 al Qaeda supporters in Great Britain, Her Majesty's government tasked the Security Service – MI5 – both to dismantle jihadist networks and devise a plan to win the hearts and minds of Britain's Muslim minority. Ultimately, the Security Services balked at a difficult job for which they had no experience or clear jurisdiction. We need to do better. Fortunately, unlike our sister democracies across the Atlantic, we have time. We must not squander it.

Written Testimony Before the

United States Senate
Committee on Homeland Security and Governmental Affairs

"Homeland Security: The Next Five Years"

Daniel B. Prieto

Senior Fellow and Director
Homeland Security Center
The Reform Institute
dprieto@reforminstitute.org

September 12, 2006

Chairman Collins, Senator Lieberman, and distinguished members of the Committee on Homeland Security and Governmental Affairs, I want to thank you for inviting me to testify before you today. My name is Daniel Prieto. I am Director of the Homeland Security Center at the Reform Institute. Previously, I was Fellow and Research Director of the Homeland Security Partnership Initiative at the Belfer Center for Science and International Affairs at the Harvard University Kennedy School of Government.

My testimony today reflects my own views and analysis and does not reflect the official position of any institution with which I am affiliated.

Introduction

Since 9/11, homeland security in the United States has, in large part, been an attempt to optimize domestic assets and activities to detect, prevent, respond to, and recover from high-consequence events, either terrorist induced or natural. Obviously, there are also a number of related international components, including military action against terrorist groups; overseas intelligence and law-enforcement cooperation; and programs to detect and interdict threats among travelers, emigrants and cargo before they arrive in the United States.

Setting aside military operations and cross-border intelligence sharing efforts, our homeland security efforts in the years since 9/11 have centered on five significant areas of activity: creating new law and policy; creating new organizations; developing new strategies and plans; implementing new "consensus" programs (e.g. C-TPAT, US-VISIT, PCII); and pursuing innovative but controversial programs (e.g. the increasing use of commercial data for terrorism-related analysis, as included in the NSA domestic surveillance program and as seen in TSA's SecureFlight and DoD's TRIA).

To make America more secure in the next five years, we need to:

1. **Adapt to a changing threat environment.**
2. **Engage Society, Educate the Public and Enlist the Private Sector.** To date, we have not done nearly enough to educate the public or to engage the resources and goodwill of the private sector.
3. **Move from Tactics to Doctrine.** Homeland security strategy documents since 2001 have provided tactics, methods and processes, but have failed to articulate strategy and doctrine that provide clear guidance for implementation and goals by which we can measure progress.
4. **Ensure DHS Succeeds.** We can not afford to have a weak DHS that lacks credibility and is challenged to carry out its mandate. One of the major problems DHS has faced is weak management of a complex merger integration process. This needs to change.
5. **Get Technology Right.** While the U.S. is the envy of the world when it comes to technology, the federal government struggles to implement important homeland security technology projects and to transfer important everyday technologies into the homeland security realm.
6. **Catalyze and Govern Information Sharing.**
7. **Develop Rules for the Use of Consumer and Company Data for Counterterrorism.**

The Changing Threat

Looking at the threat environment, the world has not stood still since 9/11. At least two major factors will pose significant new challenges over the next five years.

First, WMD proliferation threats will increase. These growing challenges come from North Korea's pursuit of nuclear weapons and the push by Iran to acquire nuclear weapons capability. The involvement by non-state actors, like the A.Q. Khan supply network, in the proliferation of WMD-related technologies, weapons design, and equipment will continue to grow in seriousness. We will also be challenged by terrorists' efforts to acquire and use WMDs, a situation made more dangerous by potential cooperation between terrorists and rogue or weak states possessing WMD and related technologies.

Second, the terrorist threat is evolving and may look quite different five years from now. Al Qaeda Central is weaker today, but it is stronger as an inspirational movement to cells that are more independent, self-starting and increasingly home-grown. This is exemplified by the perpetrators of the London transit bombings and the thwarted London airline plot. Furthermore, the speed of radicalization has accelerated. Wars in Iraq and in Lebanon provide grievances that make recruitment to radical Islamist groups easier. The proliferation of alternative media outlets and terrorists' use of the internet increase exposure to propaganda and training. Finally, like Afghanistan was for Bin Laden in the 1980s, Iraq provides a theater for the next generation of terrorist leaders to train, make connections, and build reputations.

Engaging Society, Educating the Public and Enlisting the Private Sector

Educating the Public

Faced with the threats of proliferation and global terrorism, one of the most important things we can do as a country is to harness the strength and resolve of our society. The many changes we have made to the organization of the federal government, while essential, will only go so far. The British were renowned for their resolve and determination during the London blitz in World War II. Similarly, the United States will win the war on terrorism, not by force of arms, but by the resolve and resiliency of its citizens.

The inaugural National Strategy for Homeland Security argued that "the Administration's approach to homeland security is based on the principles of shared responsibility and partnership with the Congress, state and local governments, the private sector, and the American people." While the sentiment was and is correct, we have failed to execute on it. I have argued since 9/11 for the need to create a culture of preparedness. For this to happen, we need to view our citizens as the critical backbone of American resolve.

Unfortunately, too many policymakers tend to view the general public not as a source of strength, but as either victims or prone to panic. Given such a view, it is not surprising that the federal government has struggled mightily over how much information to share with the public regarding what to do in the event of terrorist attacks and how to respond depending on the nature of the threat. Too many officials fear that that too much information will frighten the public or aid our enemies.

This discussion should end. The more informed and self-reliant we are when the next attack or disaster strikes, the better off we will be.

The most persuasive recent arguments on this front come from Brian Jenkins of RAND in his new book, *Unconquerable Nation*.[1] According to Jenkins, the federal government's approach to public education and communication has "encouraged dependency" instead of "promoting self-reliance."

> "The best way to increase our ability as a nation to respond to disasters, natural or man-made, is to enlist all citizens through education and engagement, which also happens to be a very good way to reduce the persistent anxieties that afflict us. We have not done this... We need to aggressively educate the public through all media, in the classrooms, at town halls, in civic meetings, through professional organizations, and in volunteer groups. This means more than speeches in front of the American flag. The basic course should include how to deal with the spectrum of threats we face, from "dirty bombs" to natural epidemics, with the emphasis on sound, easy-to-understand science aimed at dispelling mythology and inoculating the community against alarming rumors and panic."

Proposals on Public Education

- Significantly improve the quality of ready.gov so that it contains detailed and deep information on threats, preparedness, and response. To the extent that budgets are limited, ready.gov need not develop information on its own, but should act as a portal that

[1] Brian Michael Jenkins, *Unconquerable Nation: Knowing Our Enemy, Strengthening Ourselves*, RAND Corporation, 2006. For another excellent treatment of the topic see Amanda J. Dory, *Civil Security: Americans and the Challenge of Homeland Security*, Center for Strategic and International Studies, 2003.

organizes and consolidates links and information from sites like those of RAND and the Federation of American Scientists.

- DHS should establish an advisory board, comprising academics and scientists to ensure that materials are accurate and up-to-date, as well as experts on communications, sociology and psychology to ensure that materials are most effective at providing education that empowers our citizenry.
- DHS should increase its efforts to support homeland security education and outreach by trusted public information outlets, including the Red Cross, state and local authorities, and media outlets.

Enlist the Private Sector[2]

Since 2001, the Administration and Congress have repeatedly stressed the critical importance of "public-private partnerships" to make the country safer. Five years after 9/11, such partnership is more hope than reality.

The federal reorganization since 9/11 has raised the difficulty and transaction costs for the private sector to work with the federal government. Information sharing between government and the private sector remains stunted. Overall investment in private sector security initiatives has been modest. The federal government has failed to provide meaningful incentives or standards for securing critical sectors that pose the highest risk and where voluntary efforts have proven to be insufficient. The private sector has not been effectively integrated into response and recovery planning for major disasters, though some promising public-private initiatives have been piloted.

In short, the capabilities, assets, and goodwill of the private sector to bolster our homeland security remain largely untapped. To make America more secure, the federal government urgently needs to provide better leadership on homeland security issues and become a more active partner with the private sector.

When addressing these problems, policymakers should remember that the government is a major market player whose actions can and will affect the ability of the private sector to invest more in security. For its part, the private sector is not just a target, but also an important source for information, assets, and capabilities that the government does not possess.

Policymakers must learn how to harness the deep patriotism and sense of civic duty felt by many American business leaders. American companies are willing to commit their time, expertise, and resources to support the homeland security mission. The federal government must make a concerted effort to recognize and encourage such actions as part of a successful partnership between the federal government and the private sector.

Government engagement of the private sector would preferably be non-regulatory. But, when policymakers and the public feel that voluntary efforts by companies do not achieve adequate security, lawmakers and regulators should make sure to use all of the policy tools at their disposal. Federal standards can provide guidance and help ease industry fears of liability should their security efforts be defeated by a terrorist attack. Tax incentives can make security projects more economically feasible. Finally, Washington must realize that government regulation is not always in conflict with the best interests of the private sector. In many instances, federal action

[2] For a fuller discussion see Steven E. Flynn and Daniel B. Prieto, *Neglected Defense: Mobilizing the Private Sector to Support Homeland Security*, Council on Foreign Relations, March 2006.

can help to bound market uncertainties, making it easier for markets to work and for the private sector to make investment decisions.

Proposals on the Private Sector

- Washington needs to change its policy paradigm regarding the private sector, which, in effect, tells companies to protect themselves. On critical infrastructure issues, Washington needs to provide leadership, not followership.
- Washington must move beyond talking about the need to dramatically improve information sharing with the private sector and hold government officials accountable for actually doing it.
- DHS must strengthen the quality and experience of its personnel. One way to aid in this effort could be to establish a personnel exchange program with the private sector.
- Congress and the administration should work closely with industry to establish security standards and implement and enforce regulations where necessary and, especially, where industry is seeking standards and regulation.
- Congress should establish targeted tax incentives to promote investments in security and resiliency in the highest-risk industries.
- Congress should establish federal liability protections for companies that undertake meaningful security improvements.
- Homeland security officials should substantially increase the number of exercises for responding to catastrophic events. Private sector assets and capabilities should be fully integrated into these exercises, with a view to achieving deeper private sector integration into national and regional emergency response plans.
- Federal response plans should identify specialized supplies/capabilities that will be in short supply following certain types of terrorist incidents or high-consequence events and work with the private sector to ensure the availability of critical supplies and capabilities.
- DHS should establish a federal awards program, modeled after the prestigious Malcolm Baldridge National Quality Awards program, which recognizes private sector achievement and innovation in homeland security.

Move from Tactics to Doctrine

While over a dozen homeland security "strategy" documents have been produced since the 2001, most of them are simply discussions of tactics, methods and processes. This early generation of intended guiding documents generally fails to provide true strategy and doctrine. True strategy documents would clearly set forth priorities, provide definitive guidance for action, and establish goals against which activities and programs can be measured.

In the absence of compelling strategy, too many homeland security programs are ad hoc, reactive, and do not contribute to a coherent vision. In the next five years, tactics and standalone programs must give way to doctrine. This is particularly true in the areas of preparedness and critical infrastructure protection.

Preparedness Doctrine

According to Paul McHale, Assistant Secretary of Defense for Homeland Defense, the United States should assume that we will continue to face traditional military challenges from nation-states and that terrorists will attempt multiple simultaneous mass-casualty CBRNE attacks against the U.S. homeland.

Based on that assumption, the United States should develop a doctrine of homeland security preparedness not unlike prevailing U.S. military doctrine for most of the last 50 years. That doctrine required U.S. military forces to be prepared for two near-simultaneous wars in different theaters. A similar doctrine for homeland security would require the U.S. – DHS, other federal agencies, the National Guard, NORTHCOM and state and local entities – to be prepared to address two to three simultaneous high-consequence events, of the kind envisioned by the fifteen DHS National Planning Scenarios.

Once such a doctrine is established, it would have immediate ramifications for planning.

It would suggest, for example, greater and more specialized training for the National Guard, which has increasingly become the "Swiss-army knife" of homeland security. Creating National Guard "Special Forces" for homeland security would require Guardsmen to receive specific training against certain threat scenarios. Such specialization could occur on a regional basis, depending on event likelihood in a particular geography. For example:

DHS National Planning Scenario	**Geographically Based Training**
Scenario 1: Nuclear Detonation – 10-Kiloton Improvised Nuclear Device	National Capital Region, New York
Scenario 6: Chemical Attack – Toxic Industrial Chemicals	New Jersey
Scenario 9: Natural Disaster – Major Earthquake	California
Scenario 10: Natural Disaster – Major Hurricane	Florida
Scenario 14: Biological Attack – Foreign Animal Disease (Foot and Mouth Disease)	Texas, Missouri, Oklahoma, Nebraska

Improved training, greater specialization, a more sharply defined homeland security mission and free for-credit education at public state universities could provide a powerful incentive and improve recruiting, retention, and morale in the National Guard and Reserve. Training could also leverage existing DHS university centers of excellence.

A second implication of such a homeland security doctrine might be that NORTHCOM would better be able to address multiple simultaneous disaster scenarios if they had their own dedicated resources. They are currently only allocated 1,000 permanent personnel and $70 million. Compare that to DOD's budget in 2004 of approximately $400 Billion and 1.4 million active duty personnel.

In addition, it would be valuable to increase the level of joint training and exercises between National Guard, NORTHCOM, and state and local officials to address specific scenarios.

Proposals on Preparedness

- Establish a homeland security analogue to the military's two-war doctrine.
- Create National Guard Special Forces, providing specialized and regionally-based training against the fifteen DHS National Planning Scenarios.
- Dedicate resources to NORTHCOM.

Critical Infrastructure Doctrine

On critical infrastructure protection, the Homeland Security Act requires DHS to identify priorities, develop a comprehensive national plan, and recommend protective measures.

The latest version of the National Infrastructure Protection Plan (NIPP) fails to meet these requirements. The NIPP identifies obvious, if important tactics – public-private partnership, information sharing, and risk management – but fails to provide the kind of strategic guidance that can coherently guide resource allocation and programmatic activities. We continue to lack a comprehensive strategy for critical infrastructure that meets the requirements of the Homeland Security Act.

Our critical infrastructure efforts suffer from a number of other shortcomings.

First, DHS assumed that the market would provide sufficient incentive for companies to adequately protect critical infrastructure. That has not happened. Washington needs to step up to make sure that we protect critical infrastructure better.

Second, DHS was not granted new authorities, other than what it inherited from legacy offices, for security over vital critical infrastructure sectors. Pending legislation to grant DHS authority over the security of some segments of the chemical industry is a step in the right direction, but more needs to be done. DHS needs to be given authority over security activities at any infrastructure sites that threaten large-scale casualties or are critical to the functioning of the U.S. economy, regardless of sector. So, for example, DHS should have the authority to regulate critical energy infrastructure sites in order to mitigate known vulnerabilities in the electric grid.

Third, Washington has fallen into a kind of "political correctness" over critical infrastructure, as if all sectors pose equal risks. They do not. We must come to consensus on which sectors are more important than others. HSPD-7 started in this direction when it recommended prioritizing critical infrastructure that would have WMD-like effects if attacked. Secretary Chertoff also moved in the right direction when he talked about the importance of risk-based allocations for grant funding. But the failure to definitively establish and articulate clear priorities has been evident in DHS' miscues over the national critical infrastructure database and reductions of grant funding to Washington, DC and New York.

Prioritization of CI sectors should be based on:

- Vulnerability and Consequence. What industries best provide the terrorist trifecta: bodies, symbolism/theater, and economic impact?

- Companies' Ability to Address Vulnerability. Some industries are more capable than others of implementing significant security enhancements on their own and in the near term. The industries least able to protect themselves are those: 1) that exhibit low growth, low profit margins and tight cashflow, all of which limit capital available for investments; 2) whose businesses rely on long-lived capital assets, which are difficult to retrofit or replace easily; and 3) that are not tightly regulated and, therefore, lack a quick mechanism by which the government can simply mandate greater security.

In my judgment, these criteria indicate that the top priorities for critical infrastructure protection are chemical facilities; transportation, including airlines, ports, mass transit, and hazmat transport; and energy, including oil, gas, and the electric grid.

Further critical infrastructure prioritization should also give significant consideration to the geographic location, concentration, and interconnectedness of critical infrastructure.[3]

Fourth, DHS has sharply curtailed its critical infrastructure efforts so that it is now acting largely as a coordinator for the efforts of other agencies. This is a mistake, and in my view fails to carry out the mission Congress and the public expected. In 2004, DHS directed $300 million to critical infrastructure protective actions, including pilot programs, technology applications, bombing prevention, security training and community security planning. In FY07, only $30 million was requested for protective actions, a reduction of 90 percent in three years.

Fifth, the Federal government is failing to use all available policy tools at its disposal to enhance the security of critical infrastructure. It has generally painted a false choice between private sector self-protection and business-harming regulation. The government has failed to creatively use tax policy to promote additional security investments to the extent that it believes that industry, on its own, is not investing enough. Take for example the chemical industry. Often derided as negligent when it comes to security, major chemical manufacturers have spent $3 billion since 9/11 to enhance security, hardly evidence of negligence. If society believes that more security is warranted, the government should catalyze greater investment by providing tax incentives that make security projects more attractive. Had such tax breaks been provided to the chemicals industry soon after 9/11, the legislative debate over "inherently safer technologies" would not have been so protracted, because, I believe, many more companies would have already pursued such projects.

Improving the security of critical infrastructure is essential to the security of the country. Better yet, security investments can benefit the overall health and functioning of critical infrastructures. This helps the U.S. economy and society over the long term. Such "positive externalities" should not be overlooked as the government considers policies to catalyze greater levels of investment in infrastructure security. While our global economic rivals China and India invest scores of billions of dollars into the transportation, energy, and communications infrastructure that will power their economies for a generation, the United States makes due with decades old infrastructure that is brittle and in poor health.

The American Society of Civil Engineers in 2005 provided a national report card on the health of U.S. infrastructure.[4] With an average grade of "D" for aviation, bridges, dams, energy, rail and transit, among others, these infrastructures are more vulnerable to terrorist attack or natural disasters than we can afford, and they will have a harder time recovering after an event.

It is important to remember that the U.S. interstate highway system was built for security reasons and that the Defense Department was responsible for building the precursor network to the internet. Security considerations have always played a significant role in national investments in infrastructure. There is no reason that the same should not be true today.

Proposals on Critical Infrastructure Protection

---

[3] Paul W. Parfomak, "Vulnerability of Concentrated Critical Infrastructure: Background and Policy Options," Congressional Research Service, December 2005. For an excellent discussion of risk analysis as well as a ranking of the terrorism risks faced by individual U.S. cities see Henry Willis, A. Morral, T. Kelly, and J. Medby, *Estimating Terrorism Risk*, the RAND Corporation, 2005.

[4] American Society of Civil Engineers, *Report Card for America's Infrastructure*, 2005. Available at http://www.asce.org/reportcard/2005/index.cfm.

- Quickly come to consensus on critical infrastructure priorities.
- Use all policy tools available, including a mix of tax incentives, assistance in setting best practices, and smart regulation.
- Grant DHS sufficient authority where it is lacking, not only in chemical security but on facilities that are truly critical at a level of national significance.

Managing DHS for Success

In the next five years, it is critical to stabilize and strengthen new homeland security organizations, especially the DHS. DHS represents a large-scale merger of many agencies in addition to a number of start-up activities. The ability of DHS to manage the integration of these efforts and ensure that the whole of DHS is greater than the sum of the parts relies on a strong and experienced management cadre and the creation of a unified culture. The U.S. Government Accountability Office (GAO) rated the management challenge facing the department as "high risk" and noted that the successful transformation of a large organization takes from five to seven years. In the private sector, large-scale mergers can take three to five years to work out. Given a much less dynamic government environment, GAO's estimate may be an underestimation.

The birth of DHS has not been easy. For its successes, DHS has suffered significant failures and missteps, which in my view have seriously damaged its credibility. Katrina was its lowest moment, but it has been beset by a number of public missteps on critical infrastructure protection, grant funding, financial management, contract management, and technology; the repeated and frequent missing of Congressional deadlines; high turnover among senior staff; limited expertise among professional staff; difficulty in creating a professional cadre in important areas due to large-scale outsourcing of key strategy and integration tasks to outside contractors and an over-reliance on detailees who maintain loyalty to their home organizations; and general problems of coordination between DHS' disparate parts.

Ineffectiveness or immaturity has led to the subsequent devolution of key functions that DHS inherited only a few years ago. DHS has increasingly diminished, spun off, or shed responsibilities in such areas as intelligence and information fusion, critical infrastructure protection, and post-disaster housing and health. In the most recent federal personnel survey, DHS employees ranked their organization at or near the bottom on nearly every measure of effectiveness. Other departments – Justice, State, DoD – too often do not view DHS as a peer organization.

DHS is falling behind, and the window of opportunity to get things right may be closing. While DHS has made progress in rationalizing many basic operations, too much of DHS lacks strong management and adequate coordination. In the next five years, DHS must resolve key management issues, cease being an umbrella organization, and become a unified enterprise.

If DHS fails to create synergies among the many entities it inherited and to mature into a more effective organization, we will be worse off as a country. If it continues to receive highly critical reviews from its own inspector general and the GAO and unflattering portrayals in the press, if its employees continue to suffer from low morale and confidence in their agency, if it continues to shed key functions with which it was entrusted, and if its fails to improve its reputation among counterpart agencies, then the DHS risks becoming the DMV of the federal government: widely viewed as inefficient and ineffective. Worse yet, criticism of DHS becomes self-fulfilling. The more negatively viewed the organization is, the less effective it becomes.

Presentation of these facts is not meant as an indictment of DHS. Many of the problems were to be expected in a merger integration exercise as large and complex as DHS. My point in raising them is to urge this Committee to do all it can to shepherd the maturation of DHS. It may be necessary to read between the lines when senior DHS officials state that they have all the resources and capabilities they need, rosy scenarios which may be born of political expediency or pride. It also may be necessary to moderate a growing desire to withhold or cut DHS funding as a punitive measure. To the extent that DHS' shortcomings stem from under-resourced or structurally weak management, it is essential to not just use sticks, but to also address the root of the problem by helping strengthen management capability and accountability for the long term.

To improve DHS management, key CxO level positions must be given greater power and more resources. The Chief Financial Officer (CFO), the Chief Information Officer (CIO), and the Chief Procurement Officer continue to lack effective department-wide purview and authority. Some changes implemented by Secretary Chertoff have helped, in particular the creation of a Policy Office and an Office of Strategic Plans, as well as increasing the power of the Deputy Secretary. But an organizational chart that has 22 separate divisions reporting directly to the Deputy Secretary while failing to fully leverage the CxO positions does not make sense. Management control and integration of DHS, in my view, remain far too weak.

Congress plays an important role in DHS management as well, acting in an equivalent capacity to a board of directors. The creation of permanent homeland security committees in both the House and Senate reflect an important step in streamlining Congressional oversight. Katrina provided a galvanizing event that has allowed Congress to be much more assertive on homeland security in this past year. Reports on Katrina as well as bills on ports, borders, chemical security, FEMA, domestic surveillance, and foreign investment in critical infrastructure all demonstrate growing Congressional leadership and assertiveness. Finally, homeland security efforts in this Congressional session appear both more bipartisan and bicameral.

While these are all steps in the right direction, more needs to be done to ensure that Congress provides efficient and effective oversight of DHS' security-related components. For example, the Senate Homeland Security and Governmental Affairs Committee was not given jurisdiction over several key components within DHS, particularly as regards transportation. As advocated by the 9/11 Commission, the Senate and the House homeland security committees should have jurisdiction over all counterterrorism elements of DHS.

Proposals on DHS Management

- Significantly strengthen the DHS management directorate organizationally and with additional resources and deeper experience. Continue to build and strengthen the DHS Policy Office and Office of Strategic Plans.
- Increase coordination between the management directorate, Policy Office, and Office of Strategic Plans, and clearly empower a core "SWAT" team responsible for all integration-related issues and initiatives. Increase working-level interactions between personnel from the offices of Management, Policy, and Strategic Plans with personnel from DHS operating units. More joint interaction on projects and more open dialogue will help build trust, better enable integration-related projects, and establish stronger influence of the DHS Secretariat.
- Continue to streamline Congressional oversight and fully empower Senate and House homeland security committees to have full oversight over all security-related components of DHS.

Getting Technology Right

America is the envy of the world when it comes to technology, but too many homeland security technology projects since 9/11 have faltered, from the FBI's virtual case file and DHS' Homeland Security Information Network to border security systems. We need to better use technology and innovation to protect America. This is true not only on next generation projects like CBRNE detection, but also on migrating mass-market technologies like digital maps and online marketplaces into the homeland security arena.

Outside of the military realm, the federal government is not good at managing technology projects. Too many in government still view IT as obscure work divorced from policymaking and far less important. As a result, government tends to treat the management of technology projects as an afterthought, rather than viewing it as integral to policymaking. In the 1990s, the private sector transformed itself by learning how to deploy advanced technology strategically. The federal government needs to catch up.

While the government in general struggles to implement technology projects successfully,5 DHS is among the worst performers. According to the GAO, DHS is currently pursuing around 17 high-risk technology projects, of which 15 are suffering performance shortfalls. The 88 percent shortfall rate of DHS high-risk projects is dramatically worse than the average government shortfall rate of 35 percent.

Adding to the homeland security technology problem, the DHS Science and Technology (S&T) directorate faces significant challenges. Weak management and leadership, staffing problems, the absence of coherent long-term strategy, and financial problems have lead to proposed cuts in its budget and calls for its reorganization.

To keep the country safe, we need to make a serious and sustained effort to improve how we deal with homeland security technology. While everyday consumers have benefited significantly from the technology and telecommunications revolution of the late 1990s, the federal government has been left behind. We must recognize the power of technology to solve some of homeland security's most intractable problems.

Take for example, the need to provide better situational awareness to crisis managers, first responders, and the public. A post-Katrina DHS review of state emergency plans, found that most mass evacuation plans remain inadequate and "are an area of profound concern."

The mass market has rapidly adopted digital situational awareness products over the last five to ten years, including online maps with satellite imagery and GPS-based systems in our phones and cars. Think Mapquest, Google Maps, and OnStar. It is not acceptable for the men and women who protect the homeland to be stuck in the dark ages, nor the public they are tasked to help defend.

---

[5] See David Powner, *Information Technology: Improvements Needed to More Accurately Identify and Better Oversee Risky Projects Totaling Billions of Dollars,"* GAO-06-1099T, Government Accountability Office, September 2006. According to the GAO, approximately 300 projects totaling about $12 billion in estimated IT expenditures for fiscal year 2007 have been identified as being either "poorly planned or poorly performing." Specifically, of the 857 major IT projects in the President's budget for fiscal year 2007, OMB placed 263 projects, representing about $10 billion on its Management Watch List. In addition, in response to OMB's memorandum, agencies reported that 79 of 226 high risk projects, collectively totaling about $2.2 billion, had a performance shortfall.

Situational awareness requires a common geographic frame of reference for everyone involved and that can be easily updated as event details become clear. What evacuation and supply routes are open, closed, or destroyed? Where are essential supplies, industrial facilities and oil, gas, electric and communications lines? Where are shelters, hospitals, and churches and are they full? In a real-time terrorist event, such as a dirty bomb or chemical release, knowing whether to go east or west a few blocks can mean the difference between life and death.

To be fair, DHS has realized that good maps are essential to good disaster preparedness and response. Unfortunately, its efforts have fallen short. In 2003/4, DHS launched the Homeland Security Information Network to better communicate with state and local officials. Robust mapping capabilities were to be among its key features. But that functionality ran into trouble and delays almost immediately, and in 2006 the DHS Inspector General found that fewer than ten percent of all users were using the system on a regular basis, in part because it failed to provide useful informational awareness.

It is no surprise then that military resources were called into action by DHS during the response to Katrina. But Homeland Security should not have to beg, borrow and steal from others when it comes to their situational awareness. First-rate digital maps should not be "in case of emergency break glass." Such capabilities should be in the basic toolkit of homeland security professionals, and they should be readily shared with first responders and state and local officials.

Just as important is empowering the public with geographic situational awareness so they can better plan and make decisions at times of disaster. As we saw in New Orleans, the public is frequently on its own in the immediate aftermath of a disaster, and empowering individuals to create and share response plans with their families or co-workers remains a terribly unmet need.

To ensure that the public benefits from better situational awareness as well, all major print, online and broadcast media should agree on a single map strategy for informing the public before and during an emergency, eliminating duplication of efforts and ensuring as consistent and accurate of an information flow as is possible. Additionally, DHS could establish local "map czars" who are empowered to cut through the bureaucracy to decide what is presented on such maps, including rapidly changing information during a crisis.

Another area where technology could be used much more effectively is in inventorying and coordinating the supply and delivery of disaster response assets. According to a recent report commissioned by the White House after Katrina, the "Achilles' heel" of our national preparedness is the ability, among all those players, to identify critical supplies and resources before a disaster strikes and finding and delivering them quickly afterward.

Everyday technology, properly harnessed, can help address some of the most glaring deficiencies identified by the White House study.

Future disasters envisioned by the Department of Homeland Security will all require specialized response resources, many of which the government will not be in apposition to supply. Federal, state and local governments should identify critical supplies and capabilities – vaccines, ventilators, generators, electric transformers, laboratory capacity, decontamination equipment, logistics, transport, warehousing – that they will need ahead of time.

Building an eBay-like online market mechanism to match regional and national-level disaster-response needs with companies that can pledge assistance ahead of time or help out in real time

would save dollars and lives. Properly built and maintained, it would ensure that the vast majority of private pledges and donations are put to good use, instead of going unused, as happened in Katrina. It would allow state, local and federal governments to inventory available critical assets rapidly and would be much faster than relying on government bureaucrats to create a resource database on their own. Such a system would also serve as a focal point for cooperation between government, the private sector and NGOs. It would allow the establishment of significant cooperation, trust, and interaction in advance of the next disaster so that we are better prepared when the next disaster hits.

Proposals on Technology

- Make it an urgent priority to stabilize and strengthen DHS technology efforts and the S&T directorate. Recruit and build a strong technology management team with a multiyear commitment, and better align S&T activities with the strategic priorities of the DHS.
- Establish a panel of experts, primarily from industry, to advise the Secretary of Homeland Security on technology issues and ongoing technology projects.
- Improve situational awareness by greatly expanding the availability of digital imaging and map capabilities to homeland security professionals as well as to the public directly and via media outlets.
- Drive preparedness with internet based market mechanisms that make it easier to inventory and secure critical response assets from non-governmental actors.

Information Sharing and Counterterrorism Use of Commercial Data

Information Sharing

The President and the Congress have taken bold policy, legal and institutional steps to improve information sharing. Congress enacted the Intelligenec Reform and Terrorism Prevention Act, the President issued Executive Orders to create an Information Sharing Environment (ISE), and new organizations have been created, including the ISE Program Manager within the Directorate of National Intelligence as well as offices and boards focused on privacy and civil liberties.

The ongoing debate over intelligence collection within the United States signifies the challenge to simultaneously protect civil liberties and achieve increased security in an age when governments need more and better information in the face of dynamic and often asymmetric national security threats, as well as communications technologies and globalization which blur traditional notions of national boundaries.

While the information sharing reforms undertaken in the first five years since 9/11 are impressive, they are only a first step. On their own, they are sufficient neither to bring about the needed changes in behavior nor to build the technology systems that are needed to enable better information sharing. To move forward effectively, the government must implement policies to overcome the significant cultural and bureaucratic hurdles that impede information sharing. Better policies, clearer rules, and more robust oversight for sharing intelligence information make us more secure both in our Constitutional rights and against terrorist threats.

To ensure that policy reforms fully translate into changed behavior within critical agencies and departments, leadership from the highest levels of government is necessary. These leaders, including the President and the Director of National Intelligence, need to identify the policies,

rules, procedures, and incentives/disincentives that will promote information sharing and foster the creation of an environment of policies, business rules and technologies that will support it.

Sharing information must become part of the DNA of our intelligence, national and homeland security, and defense communities. It must be woven into the fabric of department and agency cultures, bureaucratic behavior, and standard operating procedures for intelligence and law enforcement, into the education and training of government officials, and into the technology systems that these stakeholders use every day.

Proposals on Information Sharing

I strongly recommend that the U.S. implement the many recommendations of the Markle Foundation Task Force regarding information sharing, including the innovative recommendations of the most recent report.[6]

- Adopt an authorized use standard to protect civil liberties in the sharing and accessing of information the government has lawfully collected; this standard would replace existing outdated standards based on nationality and place of collection.
- Take a "risk management" approach to classified information that better balances the risks of disclosure with the risks of failing to share information.
- Create a government-wide dispute resolution mechanism to facilitate responsible, consistent, and lawful information sharing.
- Develop tools, training, and procedures to enhance the use of the information sharing environment and its technological capabilities by line analysts and by senior officials.
- Expand community-wide training, modern analytic methods, and new tools to enhance the quality of information sharing and analysis.
- Encourage the use of new technologies such as anonymization, and the use of expert and data directories.
- Employ immutable audit systems to facilitate both accountability and better coordination of analytical activities.

Reaching Consensus on the Use of Consumer and Company Data for Counterterrorism

In May 2006, it was revealed that the NSA was augmenting domestic surveillance with large-scale data analysis of consumer telephone toll records. That revelation was only the latest instance of government efforts to use data mining and other technology techniques in the war on terror. A 2004 survey by the U.S. Government Accountability Office found 199 non-classified federal data mining projects, a number that would grow if classified projects were included.

Many of these programs have raised little controversy. Cargo security programs analyze volumes of shipper and cargo manifest data. Companies as diverse as FedEx, Western Union and AOL have been helping the federal authorities and law enforcement by allowing them to look at portions of their customer and subscriber data. Other experiments – including the Defense Department's Total Information Awareness (TIA) program and TSA efforts to use commercially-

[6] *Mobilizing Information to Prevent Terrorism: Accelerating Development of a Trusted Information Sharing Environment*, Third Report of the Markle Foundation Task Force, June 2006. *Creating a Trusted Information Network for Homeland Security*, Second Report of the Markle Foundation Task Force, December 2003. *Protecting America's Freedom in the Information Age*, First Report of the Markle Foundation Task Force, October 2002.

available consumer data in airline passenger screening – raised public outcry and privacy concerns and were shut down by Congress.

There is ongoing controversy over the government's use of private sector and consumer data for counterterrorism purposes. While privacy advocates cry foul, many Americans see little problem. A Washington Post-ABC News poll following the revelations about NSA "data mining" found that 63% of Americans supported the program.

The growth in data analysis efforts marks the recognition of a simple truth: our spies are not well suited to address the jihadist terrorist threat. We are short on Arabic language skills, community ties, and cultural knowledge that would allow our spies to infiltrate increasingly independent and decentralized cells. How, for example, would an American spy ever hope to penetrate a group like the home-grown London subway bombers? Faced with that reality, the growing use of data-analysis techniques to fight terrorism makes sense.

At the same time, government programs that analyze commercial data are imperfect and risk the wrongful entrapment of innocent citizens along with legitimate terrorists. That risk is magnified by the fact that the laws governing these programs are unclear. To the extent data is mishandled, misused or leads to false positives that are difficult to redress or correct, confidence in government is eroded.

Furthermore, the lack of a crystal clear legal framework to govern data analysis and data mining programs puts government intelligence professionals at risk. It makes intelligence officials more likely to mistakenly violate individual civil liberties and privacy laws, making them more vulnerable to lawsuits and accusations of abuse.

We need to move beyond an environment where it seems that different executive-branch agencies are simply experimenting with large-scale data analysis techniques to see what works and what they can get away with. In the next five years, we need to move past experimentation and develop comprehensive legislation, guidelines and rules to govern the growing use of consumer and company data in the fight against terrorism.

Government's use of consumer data is currently governed by a raft of disparate and piecemeal rules. Among many others, these include the Privacy Act and the E-Government Act, the Federal Information Security Management Act, the financial Modernization Act, and Patriot Act amendments to the Fair Credit Reporting Act. Various other bills, including ones on consumer data privacy and data brokers, could add to the confusion.

Similarly, there is a risk of conflicting regimes regarding critical infrastructure information. The recently finalized Protected Critical Infrastructure Information (PCII) could very well come into conflict with the sector-specific data protection regimes contemplated in chemical (S. 2145 and HR. 5695) and port security (S. 2459 and HR. 4954) bills.

Within the next five years, balkanized rules for the government's use of company and consumer data need to be addressed. Any attempt to harmonize or create a unified regime for the use and sharing of industry and consumer data for terrorism-related purposes will need to comprehensively address the government's handling and management of data from "cradle to grave." It should address the full data lifecycle: procurement, receipt, storage, use, ability to combine with other data, sharing within government, sharing with government contractors, encryption, anonymization, dispute, and redress.

The Government's use of consumer and industry data for counterterrorism purposes will continue to grow. Clear and consistent rules to govern this activity are needed so that Americans don't have to feel that the only relationship between civil liberties and security is a zero-sum game.

Conclusion

Are we safer? At the five year anniversary of 9/11, the question is unavoidable.

In many ways the answer is yes. The U.S. has not been attacked again on U.S. soil. We have successfully degraded Al Qaeda Central and are cooperating successfully with allies to detect and thwart additional attacks. Our defenses at home are stronger. We embarked on the largest reorganization of the federal government since 1947. We have sought to improve information sharing with new laws and new institutions. We have sought to make it easier to find terrorists through the innovative use of data analysis technologies while at the same time seeking to protect our values with a the creation of new privacy and civil liberties boards and offices. Airline security has been boosted. Private chemical manufacturers have invested billions on greater security since 9/11. Nuclear plants have raised security at the behest of the Nuclear Regulatory Commission. Add to these measures a higher level of public awareness and vigilance, and in many ways we are safer.

But in many ways, we are not.

The world has not stood still since 9/11. Nuclear proliferation is a growing threat, and global jihadist terrorism is adjusting and evolving. At home, our security efforts are still very much in their infancy. The emblem of our shortcomings is Katrina, with all of the significant gaps it exposed in our leadership, preparedness, coordination, and effectiveness to deal with even widely foreseen homeland security threats. We face other significant challenges going forward. DHS struggles to meet the expectations that came with its creation. Chemical plants and ports are still not secure enough. Transit authorities can't find enough money to implement desired security measures. We lack a national consensus on priorities and our strategies are not robust, leaving us with uncoordinated programs and in a perennial state of reacting to the latest threat. A number of big-ticket homeland security technology projects have faltered. Innovative but controversial "data mining" programs to enhance security are forcing the tradeoff of liberty for security in an unnecessarily zero-sum game.

"Is it safe?" Dustin Hoffman's answer to that question in the famous 1976 movie, *The Marathon Man*, was alternately "yes, "no," and "it depends." For every area of progress, significant gaps and vulnerabilities remain. Over the next five years, we must do more and do better.

In five years time, we should all hope to see:

1. A much better educated and empowered public on homeland security issues.
2. A private sector that works in much fuller partnership with the government in protecting the country.
3. A clear doctrine of national preparedness that requires us to be ready to address multiple simultaneous high-consequence homeland security events.
4. Critical infrastructure is more secure as a result of a mix of government incentives, standards and regulations. Chemical facilities are more secure. The electric grid is less brittle. All forms of transportation, not just airplanes, are less vulnerable and attacks are more resilient. Better investments in security have improved the overall

health of American critical infrastructure. This provides long-term benefits to our overall economy and society.

5. A DHS that is a healthy and respected organization, equal to the task Americans expected of it when it was created.
6. We are doing a better job of using technology to secure the homeland. DHS is able to field top-notch technology executives, professionals, and managers.
7. Information sharing is robust and accountable.
8. The privacy debate over government's use of commercial and consumer data for counterterrorism has reached equilibrium. The federal government has greater ability to look for terrorists, but also has greater accountability for its actions.

Bill Gates, the founder of Microsoft, has said that we always overestimate the change that will occur in five years and underestimate the change that will occur in ten. While we have made progress on homeland security in the first five years, many of us are frustrated by the pace of change and what we have not yet achieved. In the next five years, we have the opportunity – in fact, we have the duty – to make every effort to ensure that America is safer and more secure. Five years from now, I hope we have exceeded our own lofty expectations.

Questions for the Record
Senate Homeland Security & Governmental Affairs Committee
"Homeland Security: The Next Five Years"
All responses are current as of the date of the hearing: September 12, 2006
Secretary Michael Chertoff

Questions from Senator Collins

1. The majority of local law enforcement entities nationwide are unable to commit the same amount of resources that the NYPD has available to it in order to prevent the any home-grown terrorist attacks.

• What steps will DHS take in order to coordinate with these smaller municipalities?

Response: The Department of Homeland Security (DHS) Office of State and Local Government Coordination (OSLGC) maintains continuous liaison with municipalities of all sizes, as well as with tribal and territorial officials. Some of the methods employed include a regular (as often as weekly during some periods of the year), topic-driven series of nationwide telephone conference calls on such subjects as grants guidance, intelligence briefings, and new DHS policies and programs. Subject matter experts are guest speakers on the calls, and questions and comments are welcomed. The OLSGC staff also maintains a regular presence at national and regional conferences of important stakeholder associations such as: National League of Cities; International Association of Chiefs of Police; National Council of State Legislatures; U.S. Conference of Mayors; National Association of Counties; etc., where DHS staff maintain personal contact with leadership at all levels of government.

2. On the panels that follow, we will hear discussion of the "home-grown terrorist" threat from multiple witnesses. In particular, Richard Falkenrath will testify, and I quote, "since September 11, 2001, most terrorist plots and attacks perpetrated worldwide have been conceived, planned, and executed by individuals who are part of the local populace and who have only limited, if any, transnational linkages to terrorist organizations abroad." In addition, on the third panel, Steve Simon will devote a portion of his testimony to discussing the differences between the Muslim communities that have spawned home-grown terrorism in European countries, and America's Muslim community.

• How can we work with the American Muslim community to prevent the radicalization of our own citizens?

Response: American Muslims and American Muslim institutions have denounced terrorism and made it clear that they support fundamental American values such as democracy, pluralism, and the rule of law. Indeed, when one considers factors such as education levels, earning power, social integration, and civic participation, the experience of Muslims in the United States, unlike their counterparts in Europe, is largely positive. This is an asset to the United States and we should take advantage of it. This does not suggest that we are not facing any threats; rather, it is recognition that for all but a very small segment of American Muslims, radicalization is not an issue – support for violent extremism is not something present in their communities. While it is often difficult to predict pathways to radicalization, there appears to be a consensus that communities whose members (a) regularly interact with government; and (b) participate in civil society are less likely to become alienated and/or isolated, which many believe is a prerequisite for radicalization. Below are some of the most important steps the U.S. government and

American Muslims can take to jointly promote this "civic engagement." The DHS Office for Civil Rights & Civil Liberties would be happy to participate in an in-person meeting to brief you and your staff in more detail.

1. **Engagement.** Like we do with other communities, USG leaders and law enforcement officials in particular should continue to meet regularly with American Muslims to hear their concerns on domestic and foreign policy. Congress also has a role to play by reaching out and creating relationships with American Muslims and consulting with American Muslim leaders as it crafts legislation and policy, thus helping American Muslims to side with, and not turn against, America and the USG. As with other communities, including American Muslims in policy discussions demonstrates that they, like all Americans, have a stake in, and the power to ensure, our nation's safety and success.

2. **Civil Rights Enforcement.** We need to demonstrate that the USG is concerned about fair and equal treatment for all people; therefore, we must continue to address concerns about government activities that affect the Muslim community, including matters such as aviation watch lists, border encounters, and allegations of racial and religious profiling. Additionally, we should continue to aggressively enforce civil rights statutes to make clear that backlash and bias crimes are un-American and will not be tolerated.

3. **Public Stances on Tolerance and Respect.** In order to counter the canard that the US is engaged in a war against Muslims or Islam and promote a sense of inclusion, senior officials should reaffirm, whenever appropriate, that American Muslims are a valuable part of this country and that the United States respects Islam. Such statements are essential in times of crisis, to diffuse tensions and prevent or de-escalate conflicts.

4. **Encourage Civil Service**. When recently asked by a group of American Muslims how they could help in the homeland security effort, DHS Secretary Michael Chertoff responded that they should encourage their sons and daughters to work for the government. Indeed, promoting civil service among American Muslims demonstrates that we want and need their help to achieve the nation's goals, and in turn reduces isolation by providing them a way to have a concrete impact on official government policy.

5. **Promote Religious Freedom.** Since the terrorist attacks of September 11, American Muslim leaders have been working to de-legitimize the use of terror as a means to achieve political change and to promote, as one American Muslim leader has stated, a culture of life and reject a culture of death. Because of our form of government and cultural values, America can provide an appropriate forum for Muslim leaders to discuss the future of their faith and develop strategies for the future in a reasoned way. This is, to a large extent, a debate between Muslims and among Muslims about the nature of their faith; moreover, it is inappropriate for the USG to entangle itself in such religious matters. It is, however, the Government's job to ensure that every person can practice their faith freely and openly.

3. One of our experts, Steve Simon, who will be testifying on a later panel this morning, believes that terrorists are committed to carrying out a chemical, biological, radiological or nuclear (CBRN) attack on the United States. Such an attack would have dramatic consequences.

• What is the Department doing to prepare for such an attack? Has the Department worked with State and local governments on consequence management plans for all major cities?

Response: DHS is charged with preventing and preparing for a terrorist attack on United States soil. Chemical, biological, radiological or nuclear (CBRN) attacks can have catastrophic effects and, as such, the Department is undertaking a number of initiatives and programs to prevent and prepare for the possibility that such an attack may occur one day.

DHS' Office of Grants and Training (G&T) strengthens national preparedness by enhancing the capacity of States, Territories, local agencies, Tribal governments, and the private sector to prevent, protect against, respond to, and recover from incidents of terrorism, natural disasters, and other emergencies through coordinated training, equipment acquisition, technical assistance, and support for State and local exercises. G&T provides grants to states and local jurisdictions, providing hands-on training through a number of residential training facilities and in-service training at the local level, funding and working with state and local jurisdictions to plan and execute exercises, and providing technical assistance on-site to state and local jurisdictions.

The goal of the G&T grant programs is to provide funding to enhance the capacity of state and local jurisdictions to prevent, respond to, and recover from incidents of terrorism involving chemical, biological, radiological, nuclear, or explosive (CBRNE) weapons and cyber attacks. G&T utilizes the National Preparedness Goal to shape National Priorities and focus expenditures. This common planning framework and the tools that support it allows us as a Nation to better understand how prepared we are, how prepared we need to be, and how we prioritize efforts to close that gap.

Additionally, the DHS Office of Infrastructure Protection (IP) works to prevent terrorists from acquiring the means to mount CBRN attack in the United States, where those means are acquired within the United State. IP works with industry and other governmental entities to ensure that chemicals that can be weaponized, fissionable material, radiological material, bio-weapons and the means to produce them remain unavailable to would-be terrorists, while other elements of DHS work to ensure these materials are not brought into the United States.

Further, IP is a supporting element in planning for and responding to a terrorist event involving a weapon of mass effect. A number of programs and elements are focused on limiting the effect of a CBRN weapon and ensuring that first responders are prepared to deal with most any eventuality. The following details a number of steps being taken by IP.

Overall IP Programs:

- Site Assistance Visits (SAVs). SAVs are visits to critical infrastructure facilities by DHS protective security professionals in conjunction with subject-matter experts and

local law enforcement (LLE) to assist asset owner/operators in assessing vulnerabilities at their facilities. After performing an SAV, DHS provides the visited site's owner/operator with a list of protective measure options for consideration.

- Buffer Zone Protection Program (BZPP). The BZPP provides funds to support the implementation of Buffer Zone Plans (BZPs) outside the perimeter of identified CI/KR sites. These plans are intended to develop effective preventive and protective measures that make it more difficult for terrorists to conduct surveillance or launch attacks within the immediate vicinity of high priority CI/KR, and increase the preparedness capabilities of the local jurisdiction(s) responsible for the security and safety of the surrounding communities. Over $13 million in BZPP grants have been provided to State and local jurisdictions responsible for the protection of chemical facilities. An additional $25 million in grants for chemical infrastructure security were awarded in FY 2006 under the Chemical Sector Buffer Zone Protection Program.

- Educational Reports. Based on data gathered from SAVs and BZPs, DHS has developed three types of educational reports for use by LLE and asset owner/operators to support their efforts in better securing CI/KR assets. Characteristics and Common Vulnerabilities reports (CVs) identify common characteristics and vulnerabilities at specific types of CI/KR. Potential Indicators of Terrorist Activity reports (PIs) provide information on how to detect terrorist activity in areas surrounding CI/KR. Protective Measure (PM) reports identify best practices and other protective measures for use at specific CI/KR types. CVs and PIs have been developed for Chemical Facilities, Chemical Storage Facilities, and Chemical and Hazardous Materials Transportation. A PM report has been developed for the Chemical and Hazardous Materials Industry. These reports have been distributed to all State Homeland Security Offices with guidance to share these reports with the owners/operators of critical infrastructure and the law enforcement community within each State, as well as Captains of the Port. These reports also will be distributed to private sector owners and operators via the Chemical Sector Coordinating Council.

- TIH Rail Security. DHS, in conjunction with DOT, is supporting a variety of efforts to improve security of Toxic-by-Inhalation Hazards (TIH) rail shipments. These efforts include studying ways to make HAZMAT rail cars less identifiable; performance of vulnerability assessments for the high-risk urban areas where the largest quantities of TIH chemicals move by rail; a DC Rail Pilot Project involving a "virtual fence" with various sensors and monitors to help secure the DC rail corridor from potential incidents involving HAZMAT; and the establishment of TIH HAZMAT teams in the DC area.

- Risk Analysis and Management for Critical Asset Protection (RAMCAP). DHS has developed methodologies for both nuclear and chemical facility owners and operators to use to assess the risks associated with their facilities and develop strategies for

mitigating those risks. Methodologies have also been developed for petroleum refineries and LNG storage. This tool, Risk Analysis and Management for Critical Asset Protection (RAMCAP), was conceived to help both industry and DHS to address two broad problems that complicate national protective efforts: first, that owners and operators assess asset risk using widely divergent approaches; and second that there is no consistent guideline for cross sector application to facilitate the transfer of risk knowledge among stakeholders.

- The National Infrastructure Simulation and Analysis Center (NISAC): NISAC provides advanced modeling and simulation capabilities for the analysis of critical infrastructures, their interdependencies, vulnerabilities, and complexities. NISAC activities fall into 5 broad categories: (1) analysis on an as-needed basis with quick turn-around time; (2) detailed analysis of infrastructures and their interdependencies; (3) risk-based decision methodology assessment, development and implementation; (4) development of the tools and data necessary to perform and improve infrastructure analyses; and (5) applied research & development in support of the next generation of infrastructure and infrastructure policy issues. Examples of NISAC modeling include:
  - Los Angeles, Chicago and Houston attack scenarios.
  - Chlorine Transport disruption effects on supply chain
  - Chemical Plant disruption effect

DHS' Office of Infrastructure Protection, under HSPD-7, is responsible for leading and coordinating the effort to secure the nation's chemical and nuclear sectors. As part of its efforts to do so, IP is leading or participating in a variety of activities that are enhancing the nation's preparedness for a potential CBRN attack such as:

Chemical Sector Programs

- Chemical Site Security Regulations. In Section 550 of the Fiscal Year 2007 Homeland Security Appropriations Bill (P.L. 109-295), Congress and the President granted DHS overarching regulatory authority over chemical facility security. Specifically, DHS was granted authority to require high-risk chemical facilities to complete vulnerability assessments, develop site security plans, and implement protective measures necessary to meet DHS-defined performance standards. The Bill gives DHS six months from the date the President signed the Bill, or until April 4, 2007, to promulgate interim final regulations implementing this authority.

  Currently, DHS is in the process of developing these regulations and has established a Chemical Site Security Task Force. As part of the regulations, DHS will be requiring risk-based performance standards to ensure, among other things, that appropriate protective measures are in place to prevent the theft or diversion of explosives and chemical weapons precursors. This should help significantly diminish the terrorists' ability to acquire some of the materials necessary for successfully carrying out a chemical weapons attack.

- Chemical Comprehensive Review Program. DHS is leading an interagency effort to conduct Comprehensive Reviews (CRs) of select CI/KR across the Nation. The CR initiative is a combined effort by the Federal government, in partnership with local authorities and owner/operators, to review existing security practices and capabilities at all levels across multiple sectors, including the Chemical Sector. Information garnered from a comprehensive review allows DHS to create a fully-integrated protective plan, response plans for both tactical and non-tactical emergency service personnel, and to address security gaps through targeted grants.

  The CR process brings together stakeholders from all levels of government and the private sector in order to leverage the many capabilities and resources available to the betterment of security in the industry and in the communities in which these infrastructures reside. The Chemical CR is led by the DHS Office of Infrastructure Protection and includes participation from the United States Coast Guard (USCG), the Transportation Security Administration (TSA), the Federal Emergency Management Agency (FEMA), the Federal Bureau of Investigations (FBI), the Environmental Protection Agency (EPA), and the National Cyber Security Division (NCSD).

  The results of the reviews will increase awareness and help secure chemical materials that have the potential to be weaponized, enhance communities' surveillance and awareness capabilities, and improve communities' response capabilities to CBRN attacks, chemical attacks in particular.

- Chemical Sector Buffer Zone Protection Program Grants Program. This grant program, which is affiliated with the Chemical CR Program, provides funds to communities to develop effective preventive and protective measures that make it more difficult for terrorists to conduct surveillance or launch attacks within the immediate vicinity of high priority chemical sector critical infrastructure targets, and increase the preparedness capabilities of the local jurisdiction(s) responsible for the security and safety of the surrounding communities. During FY06, $25 million in grant funds were made available as part of this program. Grants issued under this program are strictly risk-based and carefully targeted at creating or reinforcing specific capabilities in the communities surrounding high-risk chemical regions.

- Facility Security Assessments/Facility Security Plans (FSAs/FSPs). Pursuant to the Maritime Transportation Security Act of 2002 (MTSA), owners of chemical facilities located along waterways are required to complete Facility Security Assessments (FSAs) and Facility Security Plans (FSPs) and submit them to the United States Coast Guard (USCG) for review and approval. FSPs must include security measures and procedures for responding to security threats. All chemical facilities subject to the MTSA (approximately 238) are currently operating with approved FSPs and the USCG has completed on-site compliance inspections to verify these facilities are

operating in accordance with their respective FSP. The USCG will visit these and all facilities subject to the MTSA annually, at a minimum, to ensure continued compliance.

- Tabletop exercises. As part of DHS-IP's Exercise Program, tabletop exercises have been conducted at six high-consequence chemical facilities. The findings from these exercises are compiled in After Action Reports which serve as a basis for planning future exercises; upgrading security plans and operating procedures; and taking corrective actions. The most recent of these was conducted in conjunction with the Chemical Sector Coordinating Council, and the results of the exercise have been shared throughout the industry. Additionally, the Chemical Sector has been an active participant in all of the Top Officials (TOPOFF) Exercises, from the corporate level to the individual facility level.

- Industry Threat Briefings. DHS hosts semi-weekly unclassified threat conference calls and semi-annual classified threat briefings for private industry. These briefings, which have included participation from DHS, FBI, Secret Service, and CIA, help chemical facility owners and operators understand the threats that they are facing and facilitate the implementation of focused efforts to protect their facilities and communities from attacks on chemical facilities or otherwise involving chemicals or other hazardous materials.

Nuclear Sector Programs

- Nuclear Comprehensive Review Program. DHS is leading an interagency effort to conduct Comprehensive Reviews (CRs) of select high-value CI/KR across the Nation. Commercial Nuclear Reactors and Associated (Spent Fuel Storage) Facilities were the first to engage in the CR process. Within the past 18 months, 43 of 71 facilities have participated in Comprehensive Reviews. CRs are scheduled to be performed at the remaining sites by September 2007.

  The CR initiative, led by the IP, is a structured, voluntary, and collaborative government and private sector analysis. The purpose of the review is to explore exposure to potential terrorist attack from land, air, and water approaches, the consequences of such an attack, and the integrated prevention and response capabilities of the owner/operator, state and local law enforcement and emergency response organizations. The results are used to identify gaps, or differences between existing security and emergency response capabilities, and additional capabilities needed to address terrorist-initiated actions. The team also identifies potential enhancements or options to be considered for implementation in closing or reducing a gap.

  Federal agencies participating in Nuclear Sector CRs include IP, the USCG, the FBI, and the Nuclear Regulatory Commission (NRC).

Given the criticality of the sector, IP issued a publication "Comprehensive Reviews Yield Effective Practices for Homeland Security" in March 2006, providing a summary of the best protective security and community response measures identified during the CRs. These practices can be readily adapted for other CI/KR facilities because they are for the most part readily adaptable, low-cost measures for increased readiness and preparedness in the event of a terrorist threat or all-hazards event. The publication has recently been placed on the Nuclear Energy Institute (NEI) and Indian Point Energy Center websites.

- Comprehensive Review Outcomes Working Network (CROWN). The continued maturing of the Nuclear CR process and data collection efforts has allowed for a working network to be established by the GCC (Government Coordinating Council (GCC) and the Nuclear Sector Coordinating Council (NSCC) to analyze and more formally address gaps and potential enhancements identified in the CR process. This Comprehensive Review Outcomes Working Network, led by DHS, is an interagency effort to facilitate the reduction and/or closure of gaps identified during the original CRs by addressing potential enhancements that require collaboration of Federal, State, local and private industry stakeholders, funding, or additional research and development action. This multi-agency team consists of representatives from CNPPD, RMD, USCG, FBI, NRC, and industry partners, the NSCC.

  The Nuclear CROWN has been chartered by the GCC and the NSCC to fulfill multiple responsibilities such as to collect and analyze Potential Enhancements identified during the CR process. In coordination with additional organizations such as the Office of Grants and Training (G&T), the Directorate for Science and Technology (S&T), among others, CROWN then sorts the Gaps and Potential Enhancements into one of the following four categories: (1) taining, planning, coordination or low-cost improvements; (2) options that can be covered by existing grants (e.g. BZPP, UASI); (3) enhancements that are long-term, high-cost, or not covered by existing grants; and (4) improvements that can be found throughout the entire sector, across multiple sectors, and involve possible Federal agency requirements. Using a risk-informed and cost benefit analysis approach, CROWN will prioritize the remaining gaps and potential enhancements that need to be addressed. The Nuclear CROWN and its partners will identify existing funding mechanisms and programs that can be leveraged to address the implementation of Potential Enhancements, as well as identify CI/KR regional implications. When possible, CROWN will foster the development of new funding mechanisms and programs to address those gaps and potential enhancements not covered by existing methods.

  The Gaps and Potential Enhancements are sorted by responsible party (e.g., Federal agency, State, local emergency services, or site) and distributed to participating agencies in accordance with appropriate SBU handling procedures. Representatives of the Nuclear CROWN then follow-up with the affected stakeholders approximately

three months after the distribution of Gaps and Potential Enhancements to determine what has changed since the original CR (e.g., enhancements that have been used, grants that have been applied for, receipt of grant funds, obstacles that have been encountered, other CR-related initiatives undertaken and/or completed, etc.). CROWN will provide feedback to the GCC/NSCC and to the CR process to improve the ability of sector security partners to implement potential enhancements.

To date, the CROWN process has been initiated for eleven Commercial Nuclear Reactors and Associated (Spent Fuel Storage) Facilities throughout the country whose Integrated Protective Measures Analysis (IPMA) report have been completed and signed. The application of the Nuclear CROWN's process will continue for every nuclear facility that participates in a CR. This CROWN process will also be implemented in additional sectors that participate in the Comprehensive Review program, such as the chemical sector.

- Radiological Emergency Preparedness Program. The DHS REP program continues to perform its oversight and coordination responsibilities to ensure that State and local governments are properly prepared to ensure the health and safety of the populations immediately surrounding commercial nuclear power plants in the event of a radiological incident. Every commercial nuclear power plant conducts bi-annual preparedness exercises, which are evaluated by DHS REP and the NRC. State and local emergency response plans for communities surrounding commercial power plants are reviewed on an annual basis and the REP program provides technical assistance to these communities on an as needed basis. Currently DHS REP and the NRC are studying possible changes to existing exercise scenarios to develop scenarios that more realistically depict the current threat environment, to include possible terrorist attacks on commercial nuclear power plants. In conjunction with DHS efforts to revise the National Response Plan (NRP), the Federal Radiological Preparedness Coordinating Committee (FRPCC) is developing necessary revisions to the Nuclear/Radiological Incident Annex to the NRP.

- Nuclear Coordinating Councils and Subcouncils. The Nuclear Sector Coordinating Council (NSCC) and Government Coordinating Council (GCC) were established in October 2004 under the NIPP guidelines. Two subcouncils were created within each council to specifically address issues regarding nuclear and radiological attacks on the United States.

  The NSCC/GCC-Research and Test Reactors (RTR) Subcouncil provides a forum for developing recommendations for the best path forward for the RTR community and Federal Government activities to improve security without endangering the mission of RTRs.

  The NSCC/GCC-Radioisotopes (R) Subcouncil develops and recommends strategies that will enhance the physical security and emergency preparedness of the

radioisotope subsector under the auspices of the NIPP. Specifically, the NSCC/GCC-R identifies and recommends measures to prevent risk-significant radioisotopes from being stolen, diverted, and used in radiological dispersal devices (RDDs) or radiological exposure devices (REDs). The outcome will be to ensure that the radioisotope subsector continues to provide benefits for medical, industrial, and research applications in a safe and secure manner while protecting the public health and safety.

The following are five joint working groups formed to address radioisotope issues of mutual concern:

- RDDs/REDs
- Misrepresentation of Radioisotopes
- Physical (Security) Enhancements
- Heightened Threat and Border Closings
- Transit/Transshipment

Other DHS Programs:

- Domestic Preparedness Equipment Technical Assistance Program (DPETAP): The G&T Domestic Preparedness Equipment Technical Assistance Program (DPETAP) is a comprehensive national technical assistance program for emergency responders operated in partnership with the U.S. Army's Pine Bluff Arsenal (PBA). DPETAP provides detailed technical information and hands-on equipment operation and maintenance training to assist responders to better select, operate, and maintain their radiological, chemical and biological detection and response equipment. DPETAP Mobile Technical Assistance Teams provide, at no cost to the jurisdiction, on-site technical assistance and training to assist emergency response personnel in the operation and maintenance of their domestic preparedness equipment.

- Homeland Defense Equipment Reuse (HDER) Program: The Homeland Defense Equipment (HDER) Program is a unique partnership between the DHS' Office of Grants & Training, the U.S. Department of Energy, the U.S. Navy and the Health Physics Society. The goal of the HDER Program is to provide surplus radiological detection instrumentation and other equipment, as well as training and long-term technical support, to emergency responder agencies to enhance their homeland security preparedness capabilities. Through the HDER program, responder agencies across the nation now have access to a substantial inventory of radiological detection instrumentation and other equipment that is no longer required by the Federal government. This equipment is rehabilitated and provided at no cost to the recipient.

  The Homeland Security Commercial Equipment Direct Assistance Program (CEDAP) is operated by the Office of Grants and Training (G&T) to assist smaller communities in acquiring and using commercially available equipment to prevent, deter, and respond to terrorist attacks, as identified in state homeland security strategies. This competitive program is a direct assistance program, not a grant

program, and G&T will provide the equipment and technical assistance directly to the selected jurisdictions. CEDAP's equipment offerings include: a) personal protective equipment, b) rescue tools, c) thermal imaging, night vision and video surveillance tools, d) chemical, biological and radiological detection tools, e) information technology and risk management tools, and f) interoperable communications gateways.

• It is equally important that the public is educated on the possibility of such an attack. What do you see as the Department's role in educating the public so that people are as prepared as possible?

Response: Federal, state, local and tribal governments, the public and private sectors and the general public must work together to create the culture of preparedness. DHS has a tremendous role to play in coordinating these efforts and in educating the public on all hazard preparedness. Whether it is protecting our children in their schools, our computers from hackers and viruses, or our mail, DHS realizes our communities are on the front-line and our citizens depend on DHS preparedness guidance.

In September, DHS sponsored the third annual National Preparedness Month (NPM) -- a nationwide coordinated effort held each year to encourage Americans to take simple steps to prepare for emergencies in their homes, businesses and schools and engage in volunteer activities to better prepare their communities. NPM 2006 focused on family emergency preparedness and was coordinated by the Department's *Ready* Campaign and Citizen Corps program. The month was a great success and helped further our efforts to create a culture of preparedness in this country. This year, we expanded the effort to include regional, state and local groups in addition to national organizations and increased participation by 623 percent. A total of 1,375 groups, including representatives of every state and territory, joined the NPM 2006 Coalition and pledged to promote emergency preparedness. More than 900 events were registered on the NPM 2006 calendar maintained by Citizen Corps. This was a dramatic increase over the 175 events posted in 2004 and the 436 events listed in 2005. Events in 2006 focused on a range of individual and community preparedness subjects, including specific information and hands-on introductions to fire safety, crime prevention, emergency response and medical assistance, as well as a general overview of emergency preparedness. Organizations held fairs, trainings, preparedness summits and drills in communities across the county. Many events targeted youth, senior citizens, people with disabilities and pet owners.

Furthermore, during NPM all of our events, activities and media outreach directed Americans to www.ready.gov and 1-800-BE-READY for more information. As a result we had a major increase in traffic to both resources throughout August and September. In August, the web site received more than 9.2 million hits and over 227,000 unique visitors and in September it received more than 10 million hits and over 215,000 unique visitors. Overall throughout the NPM period we increased traffic to www.ready.gov by 99 percent. Since its launch in February 2003 the Web site has received more than 1.9 billion hits and over 24.3 million unique visitors. Traffic to our toll free phone line also increased during NPM 2006. We received more than

3,900 calls in August and more than 4,100 calls in September. September's call volume was the highest in two and a half years and an increase of 52 percent over our average monthly call volume. Since its launch the phone line has received more than 272,000 calls. During the NPM period, we filled phone orders for more than 1.5 million *Ready* brochures and more than 886,000 materials were downloaded from www.ready.gov. Since February 2003, more than 9.7 million *Ready* brochures have been requested or downloaded from the Web site.

4. One of the threats and methods of terrorist attacks that we are seeing overseas – for example, in London and Madrid – are attacks delivered by improvised explosives devices. The attacks could come by way of car or truck bombs, backpack bombs carried into restaurants or other public places or even suicidal bombers who have all subscribed to the extremist message while living with the borders or our country.

• How does the Department plan enhance its intelligence capabilities in order to detect these types of potential attacks?

Response: The Homeland Infrastructure Threat and Risk Assessment Center (HITRAC), along with our Office of Intelligence & Analysis (I&A), and Office of Infrastructure Protection (IP), immediately review and evaluate overseas terrorist attacks and captured documents in order to determine the terrorists' methods of attack and explosive device characteristics. HITRAC further analyzes the incidents to determine the effectiveness of available protective measures and security procedures, in order to assess how the terrorist may have defeated these countermeasures. HITRAC reports lessons learned from these attacks and best security practices to appropriate state, local, and tribal law enforcement authorities, and to private sector security officials, for their consideration in implementing their security plans.

• What is the Department doing to help prevent and prepare this country for terrorist attacks using these types of bombs?

Response: Beginning in 2004, the Office for Bombing Prevention (OBP), within the Office of Infrastructure Protection's (IP) Protective Security Coordination Division (PSCD), initiated and implemented programs and coordination activities supporting the prevention of terrorist attacks using Improvised Explosive Devices (IEDs).

Training
Technical training programs that provide first preventers and responders (e.g., public safety bomb squads, canine squads, and public safety dive teams) in the public and private sectors and local, state, and federal governments with a primary source from which they can obtain specialized IED prevention training via Mobile Training Teams at the requesting agency's location or at regional training centers. Approximately 200 of the following IED prevention courses have been executed:

- **IED/WMD Electronics Course:** This course is intended to introduce certified bomb technicians to current terrorist tactics, techniques and procedures (TTPs) and some of the methods being employed by international bomb squads to counter the terrorist threat. The

course has been designed in eight modular segments to give the host bomb squad the option of tailoring the course to meet their specific requirements. The course can be delivered in one of four possible formats that emphasize different skills and techniques, these are:

- Threat Assessment and IED Electronic Circuits
- Threat Assessment, IED Electronic Circuits and Disrupter Practical Exercise
- Threat Assessment and Practical Scenario Led Exercises
- IED Electronic Circuits

Upon completion of this course, participants will be able to discuss current terrorist TTPs and identify some of the additional considerations and countermeasures required to successfully defeat and prevent the use of terrorist IEDs.

- **Underwater Hazardous Device (UHD) Search Course:** This 3- to 5-day course enhances underwater search capabilities of public safety divers in support of our Nation's critical infrastructure protection plans. It includes antiterrorism mitigation procedures against underwater terrorist explosive devices.
- **IED Awareness Course:** This course covers IED recognition, Trends and Terrorism, Situational awareness (threat assessment), Suicide Bomber, DHS ongoing initiatives, and Scenario 'walk through' discussion. In addition, the course supports bombing preparedness aspects of the capabilities-based planning methodology outlined in the National Preparedness Goal, the Target Capabilities List (TCL), and the Universal Task List (UTL).

Information Sharing

The Capabilities Analysis program serves as a resource for Federal, State and local authorities through efforts such as multi-jurisdiction planning, bombing prevention information sharing, and awareness. OBP has also designed and fielded the National Capabilities Analysis Database (NCAD) as the direct analytical link to determine the nation's readiness to prevent bombings. Using critical tasks and target capabilities, DHS and its partners can systematically leverage the Department of Defense's Joint IED Defeat Organization (DOD JIEDDO) ensuring potential solutions are transitioned and applied to security gaps on a task and capability basis. The data contained in NCAD provides a baseline of capability while simultaneously informing and coordinating Federal-level bombing prevention policy and planning.

National Strategy for Bombing Prevention

OIP/OBP is also facilitating the development of bombing prevention related strategies and plans, including the Congressionally- mandated National Strategy for Bombing Prevention. OIP/OBP is working closely with its DHS colleagues and interagency partners in this endeavor and will leverage all preceding efforts toward this goal. To date, OIP/OBP has developed an initial outline for the strategy that is under review by stakeholders.

To facilitate the review process, OIP/OBP will utilize the DHS *Lessons-Learned Information Sharing* system (www.LLIS.gov). This site will also be used for secure collaboration on the outline and strategy documents, revisions and commenting from participants at the Federal, State, and local/tribal levels. Private sector stakeholders will be engaged through Sector

Coordinating Councils (SCC) with direct engagement on an individual basis. Key professional organizations such as the National Bomb Squad Commanders Advisory Board (NABSCAB), National Tactical Officers Association (NTOA), International Association of Bomb Technician Investigators (IABTI), and the International Association of Chiefs of Police (IACP), as well as the Emergency Services SCC are directly involved in this effort.

Throughout the process, preceding national strategies, the DHS Preparedness framework (e.g. NRP, NIPP, NIMS), existing goals and strategic objectives, other policies and legal mandates, and third-party critiques, such as the GAO's 2004 report on terrorism-related national strategies, will be utilized to provide a roadmap for successful implementation.

Other initiatives
OIP/OBP is also involved in other ongoing DHS protective programs. These include:

- **Buffer Zone Protection Program (BZPP):** DHS continues to assist state and local law enforcement in developing Buffer Zone Plans. The purpose of this program is to develop effective preventive measures that make it more difficult for terrorists to conduct surveillance or launch attacks using IEDs from the immediate vicinity of Critical Infrastructure/Key Resource (CI/KR) targets.
- **Underwater Terrorism Prevention Plans (UTPP):** As part of the national effort to protect our ports, OBP developed comprehensive UTPPs to support DHS's mission of Maritime Homeland Security (MHLS). The purpose of UTPPs is to develop effective preventive measures that make it more difficult for terrorists to conduct surveillance or launch attacks using explosives from the immediate vicinity of a domestic port or sub-port.
- **Multi Jurisdiction Bombing Prevention Plans (MJBPP):** OBP is developing MJBPPs to provide a method to improve coordination and reduce vulnerability to attack from IEDs within a geographic planning area. The plans will provide an organized method to catalog the security stakeholders, available resources and specific actions that may be required by multiple Federal, State or local agencies. MJBPPs will use available information from the NCAD, prior IED Awareness courses and BZPPs into a comprehensive guideline (Plan) for use by all operational decision-makers tasked to respond to an IED terrorist attack.

Promoting public awareness programs
Recent events heightened the need to advance the public awareness of national bombing prevention efforts and educate DHS constituents about programs and activities available to enhance bombing prevention capabilities. The hallmark of this effort is the National Bombing Prevention and Awareness Campaign. The Secretary mandated that the OBP develop this national campaign to achieve these goals, while simultaneously delivering training and planning programs to the participants. An official November launch event in Los Angeles, CA introduced the following goals of the proposed *National Bombing Prevention & Awareness Campaign*:

- Emphasize the importance of the bombing prevention mission within the Homeland;

- Provide information to the public and media about the Department's bombing prevention activities;
- Educate and inform relevant Emergency Services Sector constituents about bombing prevention-related training, information-sharing, and technical assistance programs available to them through the Department and other Federal partners; and
- Serve as a concurrent mechanism for Capabilities-Based Planning activities at each campaign destination (initially UASI cities).

• Because local law enforcement has a better idea on the demographics of its own cities and communities, as opposed to federal agencies, how does the Department plan to include and work with local law enforcement in preventing these potential attacks?

Response: The DHS Office of State and Local Government Coordination (OSLGC) maintains continuous liaison with state and municipal police forces of all sizes, as well as with tribal and territorial officials involved with law enforcement. Members of the law enforcement community regularly participate in OSLGC nationwide conference calls. OSLGC staff includes a veteran state trooper and former county sheriff whose main responsibility is maintaining liaison with the law enforcement community. OSLGC has partnered with the DHS Intelligence and Analysis Division to develop robust relationships with state fusion centers and Homeland Security Directors, each of whom has direct links to state and local law enforcement. OSLGC staff also maintains a regular presence at national and regional conferences of important stakeholder associations such as: National League of Cities, International Association of Chiefs of Police, National Sheriffs Association, Major City Police Chiefs, and Major County Sheriffs, to enhance our ongoing relationship and broaden our understanding of their issues and concerns.

5. The threats and challenges that our nation will be facing over the next five years will continue to require finding solutions that will enhance our homeland security while not hindering the free flow of commerce. Meeting the Department's critical mission will require not only additional resources but also more integration across the Department and with state and local first responders.

• What approach will you take to ensure the Department provides sufficient funding to address the broad spectrum of homeland security needs?

Response: It is impossible to protect every person against every threat at every moment and in every place. Therefore DHS, with finite resources and with a finite number of employees, allocates resources based on risk. Our risk analysis is based on three variables: (1) threat; (2) vulnerability; and (3) consequences. These variables are usually not equal – for example, some infrastructure may be vulnerable, but the consequences of attack are relatively small; other infrastructure may be much less vulnerable, but the consequences of a successful attack are very high, even catastrophic. DHS targets resources to mitigate the greatest risks based on analysis of available data on threats, vulnerabilities, and consequences.

As part of the annual planning, programming, budgeting, and execution process, DHS develops and uses threat and vulnerability assessments. Threat assessments, provide input and perspective on projected operating environments to help inform and prioritize program resource allocation decisions. A threat assessment identifies and evaluates multiple threat types based on various factors, including capability, intention, and likelihood of different types of attack. Vulnerability assessments identify weaknesses in critical asset areas and help identify options to eliminate or mitigate those weaknesses. In FY05, DHS finalized 5 sector modules of the Risk Analysis Method for the Critical Asset Protection (RAMCAP) project. This tool provides a means to assess vulnerabilities across critical assets that are easily communicated in consistent metrics for a consistent framework across sectors. Additionally, the Homeland Infrastructure Threat and Risk Analysis Center, established by DHS, is a national center for the integration, analysis and sharing of information regarding the risks of terrorist attacks to US infrastructure.

With information on threats, vulnerabilities and consequences, DHS decision-makers are in a better position to manage the risk of a terrorist attack by more effectively setting priorities and targeting resources. Because resources are finite, DHS will concentrate first and most relentlessly on addressing threats that pose catastrophic consequences.

DHS is continuing to build a risk management framework, which uses multiple tools to inform strategic resource decisions. Building a more detailed framework involves first developing a common taxonomy, identifying target capabilities, then assessing our gaps and redundancies. Capability gaps are being identified through an analysis of attack paths and consequence paths for different event types. This information, along with an assessment of how well different programs can contribute to closing capability gaps, will be converted into relative risk value indexes that again can be used to inform relative resource allocation decisions. Risk information is being gathered for all DHS mission programs to help build a comprehensive risk management approach and provide leadership insights into which programs help address capability gaps.

6. One of the most visible innovations of the Department has been the color-coded terrorism warning system. The use of this system has reflected the difficulty involved in trying to get useful information to the public without causing a panic or compromising counterterrorism efforts. This system is part of a larger effort to help make the public feel more secure by giving members of the public the information they need to prepare for and respond to a terrorist attack.

• What lessons have you learned from strategies like the color-coded alert system?

Response: The Homeland Security Advisory System (HSAS) has evolved throughout the history of DHS and currently includes the flexibility to assign threat levels for the entire nation, or a particular geographic area or infrastructure sector, depending on the credibility and specificity of available threat information. The HSAS is a collaborative process which takes into account current threat information and incorporates the perspectives of other federal entities (both within and outside of DHS); state, local, and tribal partners; and private sector stakeholders.

The elevation of the HSAS level to ORANGE for the financial services sector in New York, northern New Jersey, and Washington, DC, in August of 2004 demonstrates how the HSAS has matured and is an example of its flexibility to adapt to available threat information and target alerts to a specific sector. This flexibility allows DHS, local communities, and others to direct resources appropriately and reduce resultant costs where possible.

7. There has been considerable concern regarding the Department's lack of information sharing across the Department's intelligence components, but also between DHS and other federal entities as well as state and local governments. Sheriff Baca, who will be testifying on the next panel, emphasized the importance of information sharing between the Federal government and local law enforcement in his written statement. He noted that the Federal intelligence agencies "possess critical information that must be synthesized with local products to provide the clearest possible forecast of potential threats."

• What are the problems you see with sharing critical information that may identify terrorists in the U. S. and abroad?

Response: The challenges to sharing information, on terrorists in the U.S. and abroad, are characterized by several primary issues, such as protection of intelligence collection methods or tradecraft, and foreign government prohibitions agreed to by the U.S. Government on sharing of information beyond the Intelligence Community. In addition, protection of U.S. Persons information, especially for individuals who are initially suspected of connections to terrorism, is especially challenging given the need to use sensitive data as evidence in legal proceedings, while also protecting the rights of U.S. Persons who are innocent until proven guilty or eventually determined not to be subjects of interest. U.S. Persons information is of particular concern because of the challenge of culling relevant data, which could help identify terror subjects from information that federal, state, and local government entities regularly gather.

Another challenge is determining which critical information should be shared with which recipients, and the mechanism to be used. Effective information sharing across organizational and jurisdictional levels requires both confidence in the security and integrity of the sharing mechanism and trust among the individuals and organizations involved in the sharing relationship. Currently, no single, standard platform exists, which is universally accessible and trusted, to share critical information at the controlled, unclassified level. We are working with the Program Manager of the Information Sharing Environment to develop a solution to this challenge. In addition, as a Department, we are working to consolidate the methods we use to interact with our Homeland Security partners, down to a simple set of common standards and platforms. We are beginning a process to move the Homeland Security Information Network (HSIN) information sharing environment behind the DHS Extranet Gateway, which will protect this environment from Internet exposure. We are also exploring our implementation of OMB Directive M06-16, recommends allowing remote access to sensitive information only with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access.

I address other problems relating to sharing across governmental boundaries, such as lack of cleared personnel and classified transport methods, in my responses to further questions.

8. On December 16, 2005, the President issued a Memorandum for the Heads of Executive Departments and Agencies, establishing "Guidelines and Requirements in Support of the Information Sharing Environment." In this memorandum, guideline 3 deals with "Standardize Procedures for Sensitive But Unclassified Information" – or "SBUs." In March 2006, the Government Accountability Office (GAO) reported that agencies they reviewed were using 56 different SBU designations. According to the President's Memorandum, you and the Attorney General were tasked with submitting recommendations for the standardization of SBU procedures for homeland security information, law enforcement information, and terrorism information by June 14, 2006.

• Were you and Attorney General Gonzales able to submit acceptable recommendations?

Response: The Presidential Guidelines required the Secretary of Homeland Security and the Attorney General, in coordination with the Secretaries of State, Defense, and Energy, and the ODNI, to submit through the Director of the Office of Management and Budget (OMB), and the Assistants to the President for Homeland Security and Counterterrorism, and National Security, a report to the President that included recommendations for the standardization of SBU procedures for homeland security information, law enforcement information, and terrorism information. The report and recommendations were to be submitted to the President within 90 days after receiving the compiled results of an inventory from each executive department and agency of their respective SBU procedures. Senior officials from DHS and the Department of Justice, on behalf of the Office of the Director of National Intelligence (ODNI), convened and co-chaired an interagency working group to coordinate the inventory and conduct an analysis of the executive-wide SBU data, both of which were completed by March 15, 2006. In May of 2006, a preliminary report, was submitted to the Program Manager of the Information Sharing Environment (PM-ISE) for further coordination jointly with the Homeland Security and National Security Councils, and OMB, prior to submission to the President. This report, and other related interagency SBU working group products are providing the foundation for additional work on this topic and the eventual recommendations that will be provided to the President. To help further guide these effort a Guideline 3 Coordinating Committee chaired by the PM-ISE with senior-level representation from the Departments of Justice, Homeland Security, State, Defense, Energy, and Transportation, the ODNI, Homeland Security Council, National Security Council, and OMB was created. This follow-on coordinating committee activity will include completion of the Guideline 3 work in submitting SBU-related recommendations to the President.

9. According to Steve Simon, who will be testifying on the third panel today, the issuance of U.S. government-sponsored security clearances for local police officers, which he calls the "necessary first step toward sharing intelligence information," has not improved significantly.

• Given the small number of local officials cleared to receive critical threat information, how can the current state of information sharing between the Federal government and State and local governments improve?

Response: In order to improve information sharing between the federal government and state and local partners, DHS is actively working both to clear more state and local officials to access classified information and to provide more comprehensive information at the unclassified level. The Department is developing Management Directives to establish a process for determining the need to provide more clearances to state and local officials and the criteria for requesting additional clearances. We are providing cleared state and local officials with access to the SECRET collateral Homeland Security Data Network (HSDN), and also through fusion centers discussed below. I have also issued guidance to components of the DHS Intelligence Enterprise to "write for release" to state and local officials. This technique downgrades intelligence products to maximize dissemination, of reporting at the controlled, unclassified level, to state and local officials who are also key customers of the Intelligence Community.

I&A's State and Local Fusion Center support program makes the Intelligence Community's resources more accessible to our state and local partners. We are allocating personnel, resources, and systems to the fusion centers. In every fusion center where a DHS analyst is stationed, we will connect that officer to the SECRET collateral HSDN, which in turn connects to the Intelligence Community's SECRET-level network. We started this process this year and will have at least 35 fusion centers staffed by FY 2008.

Transferring DHS analysts and providing system access helps move information to our state and local partners that need it. In addition, our analysts in the field, as well as those stationed at DHS headquarters, are working to identify classified information that should be tearlined, or downgraded, for dissemination at the Sensitive But Unclassified (SBU) level. Downgrading appropriate classified information also helps to provide our state and local partners with necessary threat information. In these ways, we will improve the overall level of information sharing between federal, state, and local governments across the full range of operational missions relating to homeland security.

10. Mr. Chertoff, the days when we can take safe transportation for granted are long gone. The 9/11 attacks on New York and Washington, DC, and subsequent attacks on London and Madrid are perpetual reminders that our transportation systems have become favored targets for terrorist organizations. Should there be an attack on our ports, the United States would likely raise the port security alert system to its highest level, while investigators sort out what happened and establish whether or not a follow-on attack is likely. In the interim, the flow of all inbound traffic will be slowed so that the entire intermodal container system will grind to a halt. In economic terms, the costs associated with managing the attack's aftermath could dwarf the actual destruction from the terrorist event itself.

• Does the Department today have protocols to reestablish commerce should such a horrific incident occur?

Response: Protocols to reestablish commerce are an important part of the Security and Prosperity Partnership, Goal 9, to develop and implement a common approach to critical infrastructure protection, and response to cross-border terrorist incidents and, as applicable, natural disasters. Item 9.2.7 requires Business Resumption Planning at the border by developing coordinated business resumption protocols at the border (ports of entry) in the event of an unexpected disaster and/or increased alert levels (dual binational). These protocols are in development with both Canada and Mexico to ensure a continuity of trade at our land borders. These efforts will ensure the traffic management and communication mechanisms are in place to not only provide situational awareness to the government agencies in a time of incident but also the trade community. This will allow the government and trade community to cooperatively utilize resources effectively to ensure a steady flow of trade across the borders while maintaining the necessary enforcement regime. These protocols have been tested in joint government/trade tabletop exercises and future iterations of the plan will be tested further.

Customs and Border Protection (CBP) has participated in numerous reality-based exercises in the air, land and sea environments responding to disasters, natural or man made. CBP recognizes the need for specialized teams capable of rapid response and the ability to handle unusual and dangerous situations.

To meet this challenge, CBP's Office of Field Operations has created a Special Response Team (SRT). This team is a highly trained and mobile work unit that is fully equipped and capable of responding to a catastrophic event. The SRT can rapidly respond to critical, emergent, or unique situations requiring specialized resources, tactics, and techniques and is capable of joint interoperability throughout the law enforcement arena. SRT members are strategically located throughout the nation and can be deployed within 24 hours of notification. These highly trained and skilled CBP Officers receive an expanded course of rigorous training, which includes the necessary segments to prepare the SRT members to react efficiently during post disaster situations.

Additionally, CBP operates specialized mobile equipment that can be mobilized immediately to respond to a disaster area. This response can be coordinated with the SRT or as an independent action. The fleet includes mobile imaging equipment capable of scanning a cargo container or other objects of interest and delivers an X-Ray type image. In addition, CBP will soon operate a fleet of 60 Mobile Radiation Portal Monitors (mRPM). As of September 2006, CBP has acquired thirty (30) mRPm units which are in operation at strategic seaport nationwide.

In addition to SRTs and mobile re-deployment, CBP can re-direct CBP Officers from any location.

11. The Integrated Container Inspection System (ICIS) has been promoted by some as the answer to maritime security concerns - the ability to inspect all containers before they reach our shores. Others note the potential for security enhancements of incorporating such a program into the layered system currently in place.

• How should DHS use this project? Should it be expanded dramatically to cover all foreign ports and even be deployed domestically?

Response: The Hong Kong Integrated Container Inspection System (ICIS) pilot was launched in late 2004 and utilizes Commercial Off-the-Shelf (COTS) NII equipment to screen containers as they enter two terminal operations within the Port of Hong Kong. Containers are scanned by the Vehicle and Cargo Inspection System (VACIS) and Radiation Portal Monitors (RPM), generating radiography images and radioactivity profiles, respectively, which are linked to the container number using optical character recognition software (OCR). This data can be used locally to detect and interdict suspect materials at the discretion of the port operator. If shared with U.S. government officials, data could be used to target high-risk containers before they are U.S.-bound.

As the Hong Kong Container Terminal Operators Association (HKCTOA) begins to collect this valuable screening data, DHS will work with the Association, the Hong Kong Customs & Excise department, and the Hong Kong government to develop the policies, procedures, and response protocols to take full advantage of the investment that the Hong Kong shipping community is making to better protect maritime trade and the global supply chain.

Pacific Northwest National Laboratory (PNNL) in conjunction with Oak Ridge National Laboratory under the auspices of the Department of Energy's Megaports Initiative recently completed an analysis of a large sampling of ICIS data files supplied by the HKCTOA.

Initial findings have revealed that further work needs to be done to optimize the technology to attain technical performance levels consistent with our operational systems in the United States.

In parallel with the data analysis, CBP and the Domestic Nuclear Detection Office (DNDO) have been discussing potential implementation strategies for an integrated cargo inspection system with similar benefits to those exhibited by the Hong Kong ICIS pilot.

Although a system like ICIS has great potential, CBP needs to evaluate how the system could be used in an operational environment. The initial analysis has shown that the system integration of associating a radiological profile and a radiographic image to a specific container through the use of OCR software works relatively well. However, the full capability of the integrated system to include its corresponding operational impact on the host government has not been evaluated, as concepts of operations have not been developed.

CBP will work with the HKCTOA to ensure that the technology has performance levels consistent with our US systems. CBP will then conduct additional data analysis of the system to predict technical performance levels and operational impact. Upon completion of the analysis, CBP will engage the stakeholders at the Port of Hong Kong to discuss findings and to determine follow-on actions.

12. Secretary Chertoff, the Container Security Initiative (CSI), although well-intentioned, has serious flaws. This Committee and GAO found that only a small percentage of high-risk containers are actually inspected overseas. The touted purpose of the CSI program is to identify and inspect high-risk containers before they are loaded on vessels en route to the United States. There are some excuses for this discrepancy - such as additional information that has been received on the shipment resolving the concerns. However, that does not explain the big gap between what is assessed as high-risk and what is actually inspected. What is being done to address the gap?

Response: As part of CBP's multi-layered enforcement strategy, the Automated Targeting System (ATS) employs a risk management approach to identifying high-risk shipments. All bill-of-lading data for cargo destined for the United States are run through ATS and are risk scored. At CSI ports, those shipments deemed as high-risk are referred to the host government for additional scrutiny, using information and databases available to the host customs officials. Through this joint targeting methodology, the original risk can be mitigated due to the information supplied by the host government – information that is not available to U.S. CBP officers. Furthermore, there have been no instances where CBP domestically has found any terrorist related shipments that were missed or overlooked in CSI locations.

13. Chemical security has been a high priority for this Committee over the past two years, and it continues to be a high priority.

• In the next five years, what are your priorities for critical infrastructure protection in the United States? What critical infrastructure sectors, in addition to the chemical sector, do you believe warrant the most attention and resources to better secure in the next five years?

Response: The top priorities for the protection of critical infrastructure and key resources in the United States over the next five years include taking actions needed to build a safer, more secure and more resilient America by implementing the unified, risk-based approach described in the National Infrastructure Protection Plan. This includes: maintaining a coordinated effort to allocate resources where they will have the greatest impact for reducing risk to the Nation's CI/KR; enhancing partnership and information-sharing between a diverse set of government and private sector security-partners; and utilizing the risk management framework to:

- set security goals
- identify assets, systems, networks and functions
- establish priorities
- implement protective measures
- maintain a feedback loop that utilizes metrics to measure progress and ensure continuous improvement.

The priorities also include focusing on activities that help to sustain the CI/KR program over the long term: optimizing the utilization of technological advances through support and encouragement of focused research and development efforts; national awareness, training, exercise and professional development; and ongoing, routine management and maintenance of the National Infrastructure Protection Plan and the 17 Sector Specific Plans.

DHS identifies sectors that warrant the most attention and resources based on detailed evaluation of risk and threat. Because of the sensitive nature of this information, the list of sectors deemed to be of the highest priority based on risk is maintained at the classified level. DHS can provide this information in a separate classified document.

14. Our Coast Guard men and women have performed superbly to improve the country's port security posture. At the same time they have also responded aggressively to natural disasters and oil spills, conducted numerous vessel and facility safety examinations. In a recent Office of Inspector General report (Annual Review of Mission Performance: United States Coast Guard (FY 2005)) released in July, however, it is reported that:

> "Based on total resource hour data (provided in the report) coupled with (the) Coast Guard's limited and finite level of aircraft, cutters, and boats, the Coast Guard is within 4% of its statistically projected maximum level of resource hours. Given that resource hours are based on the limited and finite number of available assets, the Coast Guard will be unable to increase its total resource hours without acquisition of additional aircraft, cutters, and boats."

In addition, a recent Government Accountability Office audit (GAO Report on the Status of Deepwater Fast Response Cutter Design Efforts 06-764, June 2006) highlights that, due to problems with the original design, the first of these cutters "will likely not be delivered until late fiscal year 2009, at the earliest, rather than 2007 as outlined in the 2005 Revised Deepwater Implementation Plan. It seems dangerous to be operating so close to our Coast Guard's maximum resource hour level and yet components of the Coast Guard's primary recapitalization project (Integrated Deepwater Program) are being delayed. One must assume, because the Coast Guard is so close to its maximum operating level, that if we had a terrorist related incident involving a seaport, our Coast Guard would be hard pressed to meet increased security requirements without discontinuing other non-homeland security missions such as search and rescue, marine safety, and marine environmental protection.

• What is your plan to ensure that the programs already in place to recapitalize Coast Guard assets such as aging 378-foot High Endurance Cutters and 110-foot Patrol Boats are managed so that replacement assets are delivered as soon as possible?

Response: The Coast Guard is keenly aware of the need to recapitalize its aging fleet of cutters and aircraft and continues to make progress executing the Deepwater Programs Revised Post-9/11 Implementation Plan. The Post-9/11 Plan is well-aligned with the Department of Homeland Security and National strategic goals and priorities and will ensure that Deepwater Program cutters and aircraft are equipped with the right systems and capabilities to operate successfully in a more challenging post-9/11 threat environment. The Deepwater Program is now in the production phase that places a higher premium on acquisition and delivery of more capable, interoperable assets and systems. Some examples of major acquisitions in motion are as follows:

- First National Security Cutter (NSC) the BERTHOLF has been placed in the water and will be christened 11 November and delivered next year.

- The second NSC, the WASCHE, had its Keel laying ceremony on September 11.
- NSCs #3-#8 are programmed to be delivered to the Coast Guard by calendar year 2015. A total of eight Legend Class NSCs will provide the Coast Guard with a highly capable, interoperable force multiplier unlike any previous Coast Guard surface asset.
- Fast Response Cutter-A Class (FRC is programmed to replace the aging 110' Patrol Boats) design has been programmed to be delivered earlier than in the Pre 9/11 Plan. However, owing to a technical issue, the critical design review was deferred earlier this year. A Business Case Analysis for a composite hull FRC-A class is also being updated to ensure that life-cycle costs are current. Once the results are available early next year, this information will be used to determine the way ahead for the FRC-A Class design.
- Fast Response Cutter-B Class (also known as the Parent Craft) is an interim solution being implemented to help alleviate the current patrol boat mission hour gap by delivering a Patrol Boat as soon as it would be prudent. The Coast Guard has recently completed its review of the market research information obtained through the Request for Information (RFI) that was initiated by the Coast Guard in April of this year. The Parent Craft Request for Proposal (RFP) package, for Selection and Contract Design, is in final review. The Coast Guard estimate is that the RFP will be issued to Integrated Coast Guard Systems, the Prime Contractor, sometime during October 2006. The interim plan is to acquire 12 FRC-B Class cutters using an existing in-service, proven design that carries less risk while the Coast Guard completes the FRC-A Business Case Analysis.

Shortly after becoming Commandant of the Coast Guard, Admiral Allen stated that his goal for the Deepwater Program is "ruthless Execution," meaning that the Coast Guard will execute the Deepwater Program in the most effective manner possible, with proper focus on oversight, and program management, cost control, logistical support, and platform effectiveness.

• How would an increase in our maritime security level affect the Coast Guard's ability to conduct non-homeland security missions?

Response: The Coast Guard's key strength – its multi-mission nature – allows for surge response to a myriad of events, including a potential increase in the maritime security level of the nation. This is possible through a combination of the Coast Guard's military nature, the capability of its people and assets and its risk-based approach to allocating resources. However, sustaining an operational surge is always a challenge. Capacity, capability and operational tempo challenges exist, and the Coast Guard strives to ensure coverage of all mission areas through the use of risk analysis, reasoned allocation of resources and aggressive pursuit of partnerships.

15. On a typical day, your officers process over a million people who enter our country through our land, air and sea ports. This presents a significant challenge to border enforcement officers, who have a tremendous responsibility balancing the facilitation of legal movement of commerce

and individuals across our borders, while combating illegal importation and immigration. We have had to learn the hard way that individuals coming into our country are not always who and what they claim to be, making the job your officers do much more difficult, as they make their determinations of who will be allowed to enter our country.

• What kinds of improvements and safeguards have been made to ensure that front-line officers have the proper resources and intelligence to make the proper judgment calls at the border?

Response: Customs and Border Protection (CBP) uses a multi-tiered approach to ensuring that CBP Officers have the tools and expertise available to quickly and effectively ascertain the risks associated with each applicant for admission. This includes comprehensive training in interview techniques that help officers in eliciting responses, detecting terrorists, and reviewing fraudulent documents. CBP Officers are provided with tactical intelligence and operational guidance through daily musters and other sources. Our law enforcement databases significantly enhances our ability to recognize those travelers who may pose a risk to national security, may be attempting to smuggle prohibited items, or may be attempting to illegally immigrate to the United States. With the increasing collection of biometric identifiers such as digitized photographs and fingerprints and the direct linkage to various government application databases to query and match against those biometrics, CBP Officers can verify an individual's identity.

16. In a recent Executive Memorandum (#1009 dated August 7, 2006) by Dr. James Carafano for the Heritage Foundation, Dr. Carafano points out that the Secure Border Initiative (SBI) you announced in November of last year "cannot afford to focus resources only on the land borders. It must also include the strengthening of maritime and air approaches to U.S. territory." Doctor Carafano goes on to say that "Allocating resources to land-only solutions will lead to a failed border security strategy."

• How does DHS plan to integrate its border security efforts across agency lines and, in particular, how are you planning to respond to a potential increase in the exploitation of our maritime borders as a route of illegal immigration as it becomes more difficult to penetrate the land borders?

Response: The Secure Border Initiative (SBI) is a comprehensive, long-term plan to control the nation's borders and stem the flow of illegal immigration through an integrated mix of increased staffing, more robust interior enforcement, greater investment in detection technology and infrastructure, and enhanced coordination on federal, state, local and international levels. It was created to bring clarity of mission, effective coordination of DHS assets, and greater accountability to the work of DHS in securing the Nation's borders.

The challenge of securing America's land, air, and sea borders involves numerous interrelated objectives and the ongoing work of multiple DHS components. It also entails close coordination with other Federal departments, foreign governments, and State, local, tribal, and private sector partners. Four operating components at DHS have especially central roles regarding border security: Customs and Border Protection (CBP), Immigration and Customs Enforcement (ICE),

U.S. Citizenship and Immigration Services (USCIS), and the United States Coast Guard (USCG). A Secure Border Coordination Council was created and is chaired by the Deputy Secretary to ensure Departmental coordination.

• Will we be able to respond to this potential shift, without reducing other missions, given that the Coast Guard is currently within 4% of its statistically projected maximum level of resource hours as reported by the Office of the Inspector General in its Annual Review of Coast Guard Mission Performance for fiscal year 2005.

Response: Mission performance across all Coast Guard programs is constantly managed through risk analysis to optimize outcomes. The Coast Guard currently conducts patrols and monitors sensors to help assess the threat of border crossings in the maritime areas adjacent to the Southwest border. As the land border is better sealed, and if the threat indicates a potential increase in maritime crossings, the Coast Guard will re-deploy assets from areas of lower threat and from lower risk missions. However, this surge is only sustainable for the short term.

17. Since the events of 9/11, much emphasis has been placed on securing the borders of our country. The Border Patrol continues to hire at unprecedented levels, and I understand that this summer they have reached the 12,000 agent mark, with the majority of them assigned to the Southwest Border. While illegal immigration continues out of control along the Southwest Border, our entire Northern Border is being patrolled by less than 1000 agents, presenting a vulnerable situation that cannot continue. Protecting our Nation's borders against illegal immigration is important, but securing our borders against terrorists and their weapons of mass destruction is paramount, since terrorist organizations will continue to exploit our vulnerabilities.

• What is your long-term strategy for bringing the Southwest Border under control, while at the same time securing the largely unprotected Northern Border?

Response: CBP Border Patrol has developed a comprehensive national strategy to gain and maintain operational control of our borders, between the ports of entry, with the appropriate mixture of staffing, technology and tactical infrastructure.

The CBP Border Patrol strategy is a part of the Secure Border Initiative (SBI). SBI is a comprehensive, long-term plan to control the nation's borders and stem the flow of illegal immigration through an integrated mix of increased staffing, more robust interior enforcement, greater investment in detection technology and infrastructure, and enhanced coordination on federal, state, local and international levels.

A critical component of the SBI strategy is SBInet, the CBP solution to securing the southern and northern borders. SBInet will integrate the latest technology and infrastructure to interdict illegal immigration and stop threats attempting to cross our borders, both at and between the ports of entry (POEs).

As part of the National Strategy, the Border Patrol will focus on:

Southern Border:

- Achieve proper balance between personnel, equipment, technology, and border infrastructure
- Gain, maintain and expand control of borders based on threat and priority
- Enhance rapid response capabilities

Northern Border:

- Balance intelligence use, other agency liaison efforts, technology and equipment use and personnel
- Identify threat areas and resource requirements to mitigate and defeat threats
- Acquire communications and data infrastructure to support detection and response
- Expand detection technologies and sensoring platforms
- Improve mobility and rapid response capability

18. As the end of this fiscal year approaches, Customs and Border Protection is reporting that once again more than one million people have been arrested attempting to enter our country illegally across our land borders. Almost a tenth of those arrested were other-than-Mexican, or OTM's, from 148 different countries. This past year, your Department has endeavored to end the "catch and release" practice, where many of these OTM's are released into the U. S., due to the lack of bed space, as well as an immigration court infrastructure capable of handling large volumes of deportation cases. This practice, over the years, has had a demoralizing affect on the men and women to place their lives on the line to guard our borders, and has added to the large illegal alien population. I realize that a portion of this problem lies in your Department and a portion lies with the Justice Department.

• Please describe your efforts to resolve this dilemma within your department and to coordinate with the appropriate agencies and departments who have a part in this problem.

Response: The Department has successfully ended the long-standing practice of catch and release along the southern and northern borders. This was possible through the coordination of the Border Patrol, ICE Office of Detention and Removal, the Department of Justice's United States Attorney's Office (Western District of Texas), Federal Magistrates and District Court Judges, and the U.S. Marshals Service. As a result of the Administration's efforts, described in more detail below, 100 percent of illegal aliens who are apprehended are being detained for return, signaling the end of "catch-and-release" along the border

In 2005, approximately 71 percent of OTMs were caught and released along the southwest border. ICE has worked to change that. Through partnership with other DHS entities, including the Border Patrol, and under the Secure Border Initiative (SBI), ICE has reduced processing times and more effectively use the existing beds.

Specifically, ICE is achieving measurable success in making detention and removal of aliens more efficient. The expansion of Expedited Removal (ER) authority to the southern and

northern borders improved the ability to remove aliens quickly and efficiently. Authorized under Section 235(b) of the Immigration and Nationality Act, the ER process authorizes immigration officers, under certain circumstances, to formally remove certain aliens from the United States. In fact, the average length of stay in ICE custody for aliens placed in ER proceedings is approximately 19 days, down significantly from the average of 90 days for aliens placed in traditional removal proceedings before the SBI was launched.

ICE has also increased its use of the Justice Prisoner and Alien Transportation System (JPATS), allowing for the prompt transport of aliens within and without the United States on government-owned or –leased aircraft. ICE movements using JPATS, for flights both within the United States and abroad, have increased from approximately 10,000 in FY 1995 to more than 118,200 by the end of FY 2006. In FY 2006, ICE removed 49,103 aliens from the United States via JPATS flights to foreign countries.

Furthermore, ICE is expanding its use of technology to increase removal efficiency. Video teleconferencing capability has been installed at several foreign consulates, allowing foreign consular officials to promptly interview their nationals remotely, rather than in person. This eliminates the delays associated with traditional in-person interviews, making the removal process faster and easier, particularly with Honduran nationals, whose average length of stay in the United States is now just 14.87 days under the SBI.

Another example of interagency cooperation is Operation Streamline. The Del Rio Border Patrol Sector initiated Operation Streamline on December 6, 2005, and established a "zero-tolerance zone" for illegal entry. All persons entering the U.S. through this zone were criminally prosecuted for illegal entry. The operation began in one specific area less than 5 miles wide. Today, the operation encompasses the Del Rio Sector's entire 210 miles of international boundary, as well as 5,321 miles of interior zones. The overall square miles under operational focus is 5,867. As of September 2006, result of this operation, 8,118 criminal complaints have been filed, apprehensions of other than Mexican (OTM) aliens are down 86%, and apprehensions of Salvadorans are down 93%.

19. Millions of U.S. citizens ride and depend on mass transit systems everyday. While it is difficult to fully secure all aspects of every city's mass transit system, what measures can DHS take to help secure these systems and prevent an attack?

Response: DHS has consistently stated that mass transit security and passenger rail security are a shared responsibility among a variety of stakeholders, including state, local, and Federal agencies, and private owners and operators. The primary focus for the Department and the Transportation Security Administration (TSA) has been on information sharing, preparedness, domain awareness, training, and using a risk-based management approach to maximize the impact of available resources through random, visible security activities. We have employed wide-ranging strategies that engage our stakeholders and help ensure the security of mass transit and passenger rail systems. These strategies include:

- Regional Groups

- TSA Field Presence
- National Explosives Detection Canine Team Program
- Security Training
- Grant Programs
- Visible Intermodal Prevention and Protection Teams (VIPR)

Regional Groups

The creation of regional groups enhances coordination and improves communication among Federal, State, and local governmental partners and area mass transit stakeholders. This strategy has been implemented through various programs and initiatives in the past year. The creation of these groups helps to establish a forum and process for more effective communication and information exchange among various governmental agencies and public transportation stakeholders. For example:

- Through the National Infrastructure Protection Plan (NIPP), the Department has established a forum and a process for more effective communication and information exchange among various agencies and with the public transportation stakeholders. In January 2006, TSA led the formation of the Transportation Sector Government Coordinating Council (TSGCC). Among its initial actions, the TSGCC called for the establishment of coordinating councils in each of the transportation modes.
- In March 2006, TSA led the effort to organize the Transit, Commuter and Long-Distance Rail Government Coordinating Council (TCLDR-GCC). This body brings together representatives from DHS, the Department of Transportation (DOT), TSA, the Federal Transit Administration (FTA), and the Federal Bureau of Investigation in a networked, collaborative process to develop consistent and effective security strategies and programs.
- The TCLDR-GCC engaged stakeholders in the passenger rail and mass transit communities to establish a Mass Transit Sector Coordinating Council. Participating entities include American Public Transportation Association (APTA), the Community Transport Association of America, and individual transit agencies representative of the community in system size and geographic spread.
- In support of these efforts, DHS established the Critical Infrastructure Partnership Advisory Committee (CIPAC) (as announced in the Federal Register on March 24, 2006 [Volume 71, Number 57, pages 14930-33]). CIPAC provides a process for engagement between GCCs and Sector Coordinating Councils on a broad spectrum of collaborative security-related activities.
- In August 2005, the Department initiated the interagency Passenger Rail and Rail Transit Information Pilot Program. This program is aimed at knocking down bureaucratic hurdles in the handling and dissemination of information by Federal entities. It ensures decision makers at all levels have a comprehensive and accurate picture of the state of passenger rail and rail transit security, and has streamlined procedures that improve communication

and information sharing with stakeholders during both normal operating periods and emergencies. By integrating a network approach to the Federal Government entities involved in transit security, this program ensures the coordinating forums act upon timely and reliable information.

- TSA is working with DHS/G&T and DOT/FTA on developing the National Resource Center (NRC). The NRC will provide a comprehensive database allowing the transit industry to access information on a broad spectrum of subjects pertinent to transit security. Presently, this information is not readily available in any consolidated format. As an initial product of this effort, a periodic newsletter will be prepared and coordinated by TSA. This newsletter will provide items on Federal transit security initiatives; recent suspicious activity reporting with security context; and updates on model security practices observed in STSI assessments, technology programs, and other areas of interest. The newsletter will also incorporate effective security practices and items of general interest from transit agencies.

TSA Field Presence

Another key component of DHS's security strategy for rail and transit systems is TSA's field presence. This occurs through Federal Security Directors and the Surface Transportation Security Inspection program (STSI).

Through STSI, TSA has deployed 100 inspectors to 18 field offices across the country. These inspectors provide support to our Nation's largest railroads and mass transit systems performing frequent inspections of key facilities, including stations and terminals, to identify potential threats. Inspectors are actively engaged in a range of security enhancement programs, such as assessing transit systems postures in implementing core transit security fundamentals and comprehensive security action items. Inspectors also conduct systematic examinations of stakeholder operations, including compliance with security requirements; identification of security gaps; and development of effective practices. The program's consistent presence and engagement with transit system security officials fosters an integrated approach to security enhancement efforts.

Buttressing these regional efforts is an expansion of explosives detection capabilities. The Department is aggressively testing screening technologies, with an emphasis on practical use in a transit environment and mobility. These new technologies include:

- Developing and deploying chemical detection equipment in segments of the Washington, D.C., New York City, and Boston rail systems;
- Testing the movable "checkpoint" equipment, which can fit into two standard-size shipping containers and be rapidly deployed for use in screening and detection at any major system in the country in a particular threat situation;
- Developing new surveillance camera systems designed to detect human anomalous behavior for use with surveillance/closed circuit television camera systems;

- Evaluating new explosive detection equipment by field testing its effectiveness in partnership with the Port Authority of New York and New Jersey; and
- Testing a detection system in Baltimore in partnership with the Maryland Transit and State authorities to ascertain its ability to identify explosive compounds on passengers before they board a train.

By continuing these initiatives, the Department plans to identify optimal technological solutions that expand detection capabilities for explosives and chemical, biological, and radiological weapons.

National Explosives Detection Canine Team Program

Through the National Explosives Detection Canine Team program, the Department deploys three explosives detection canine teams each to 11 of the largest transit systems nationwide. Two additional systems will receive this support by the end of 2006. The TSA-trained and certified teams provide strong detection and deterrent capabilities and can be sent quickly to key junction points across systems, stations, terminals, and other facilities. This resource provides a visible and effective detection and deterrence presence in the public transportation system and can be surged to other venues as threats dictate. Teams can post at key junctions or points within systems, stations, terminals, and facilities, and deploy throughout rail systems. Random deployment heightens the deterrent effect. The Department provides funding, training, and management to the National Explosives Detection Canine Team program.

Security Training

Training and public awareness are crucial, strategic underpinnings to enhancing rail security. DHS is involved in several training initiatives, including:

- Funding several Land Transportation Anti-Terrorism Programs that provide training to local authorities in protecting land transportation infrastructure, including rail, light rail, and mass transit;
- Partnering with the Federal Transit Administration (FTA) on Connecting Communities, a series of forums to help transportation and emergency response agencies work together to prepare and protect their communities;
- Working on the development of an interactive computer-based program for both passenger and freight rail employees to provide the knowledge and skills necessary to identify security threats, observe/report suspicious activities and objects, and initiate action to mitigate, or recover from, a threat or incident; and
- Supporting the Transit Watch Program, led by FTA, which provides a nationwide safety and security awareness program to passengers and employees through both printed materials and CD-ROM format.

Grant Programs

To foster continued development of effective transit security programs, the Department administers the Transit Security Grant Program focused on rail transit, intracity bus, and ferry

systems. A network integrating the Department's Office of Grants and Training, TSA, and FTA has been established to provide assistance to eligible transit systems in completing applications for award. Both in funding allocations and priorities, this year's program reflects the Department's risk-based approach to security.

The program guidelines and application materials were recently published. Factors considered in evaluating proposals include the enhancement of capabilities to: (1) deter, detect, and respond to terrorist attacks employing improvised explosive devices; (2) mitigate high consequence risks identified in individual transit system risk assessments; (3) implement technology for detection of explosives and monitoring for suspicious activities; (4) improve coordination with law enforcement and emergency responders; and (5) expand security training and awareness among employees and passengers.

Visible Intermodal Prevention and Protection Teams (VIPR)

Additional security resources are applied through the development of VIPR Teams. VIPR teams, which are deployed randomly, add to the TSA's strategy of layered security, and introduce an element of unpredictability to disrupt potential terrorist planning activities. VIPR Teams consist of personnel from the Federal Air Marshal Service (FAMS), STSI, and explosives detection canine teams. VIPR teams were created as a way to prepare for emergency situations in which TSA assets would be invited to assist a local transit agency. VIPR teams allow TSA and local entities to develop templates that can be immediately implemented in emergency situations. FAMS participation in VIPR deployments are planned for brief periods and are scheduled not to interfere with normal aviation operations. Using advanced screening technology, these teams provide the ability to leverage a variety of resources quickly and effectively. The deployments are designed to raise the level of security anywhere in the country. The teams work with local security and law enforcement officials to supplement existing security resources and provide deterrent presence and detection capabilities.

20. Your department's science and technology (S&T) directorate, which conducts vital long-range research in areas including anti-explosives technology, received drastic funding cuts from the Senate Appropriators in the fiscal year 2007 homeland security appropriations bill. The Senate Appropriations Committee referred to the directorate as a "rudderless ship," citing poor management in their report accompanying the bill. Admiral Jay Cohen, newly sworn in as Undersecretary for Science and Technology, told my Committee staff of his management and realignment plan for the directorate, stating that he wants the structure to reflect your strategic goals as well as address some of the problems identified by the Appropriations Committee.

• Secretary Chertoff, what are your goals for the Science and Technology Directorate and how do you aim to get the "rudderless ship" on course with those goals?

Response: The S&T Directorate is improving its business approach by streamlining processes, improving accountability and empowering people. The S&T Directorate is implementing this improved business approach through its Planning, Programming, Budgeting, and Execution (PPBE) process, which encompasses the development of strategy, priorities, program plans,

resource requirements, and associated performance metrics. The PPBE process is a continual cycle that drives the organization to evaluate strategies, refine its resource allocations, and ensure that it remains accountable. Outcomes of this process will be reflected in a 5-year research and development plan that will outline our strategic direction, detail all of our R&D programs, and set out a performance measurement approach to ensure accountability.

In addition, to improving its business approach, the S&T Directorate is implementing many changes that will enable it to be a more responsive, agile, customer-focused organization – one that better enables our Nation to prevent, protect, respond, and recover from acts of terrorism, natural disasters or other emergencies. These changes include new leadership, an aligned organizational structure and further focusing the work of the S&T Directorate.

In August, the Senate confirmed Jay M. Cohen as the new Under Secretary for Science and Technology. Under Secretary Cohen brings vast scientific expertise and critical leadership to the Department having recently served as Chief of Naval Research, commanding the Office of Naval Research and managing science and technology programs for the Navy and Marine Corps.

Under Secretary Cohen has already aligned the S&T Directorate and supports a clearly defined mission for the S&T Directorate: to protect the homeland by providing Federal, state, local, and tribal officials with state-of-the-art technology and resources. The S&T Directorate will accomplish this by:

- Developing and deploying state-of-the-art, high performance, affordable systems to prevent, detect and mitigate the consequences of chemical, biological, and explosive attacks;
- Developing equipment, protocols, and training procedures for response to and recovery from chemical, biological, and explosive attacks;
- Enhancing the technical capabilities of the Department's operational elements and other Federal, State, local and tribal agencies to fulfill their homeland security related missions;
- Developing methods and capabilities to test and assess threats and vulnerabilities, and prevent technology surprise and anticipate emerging threats;
- Developing technical standards and establish laboratories to evaluate homeland security and emergency responder technologies, and evaluate technologies for SAFETY Act protections; and
- Supporting U.S. leadership in science and technology.

The S&T Directorate has a significant role in bringing to bear solutions to the Department's homeland security challenges. These and other changes will provide the Department with an S&T Directorate that is easier to access, so that homeland security personnel can utilize technologies and solutions that will make their jobs better, more efficient, more cost effective, and safer.

Questions for the Record
Senate Homeland Security & Governmental Affairs Committee
"Homeland Security: The Next Five Years"
All responses are current as of the date of the hearing: September 12, 2006
Secretary Michael Chertoff

Questions from Senator Pete V. Domenici

1. Mr. Secretary, since 2001 there have been some well-publicized foiled terrorist plots. Most recently, we were told of the plan to detonate liquid explosives on international flights between the United States and the United Kingdom. I know that for every foiled plot that makes the news, your Department is working to prevent dozens of others.

• Will you spend a few minutes talking to us in general terms about your Department's efforts over the past four years?

Response: We have begun to build a solid foundation for our future security as a nation, one that recognizes the dynamic nature of the enemy and is focused on risk management. This is not risk elimination, but it is management of risk. One of our most significant obstacles is balancing security with liberty, prosperity and the convenience and freedom that we expect as part of our way of life.

As part of the Department's maturation over the last couple years, we have dramatically improved the way we screen people at the border. We are collecting two biometric fingerprints from foreign visitors who come to the United States, and we are now moving to collecting 10 prints. This will give us, for the first time, the capability to identify the unknown terrorist, based on latent fingerprints that we pick up in battlefields and in safe houses all over the world. This is a major step forward, and something that was not foreseeable five years ago. It is also something that we have achieved without a major increase in the waiting times or any major interference with travel.

We have also dramatically improved the way we screen cargo. We now assess all incoming containers for risk and we inspect all high-risk containers. We scan virtually every container that comes into the United States from across our land border or from overseas through radiation detection equipment. DHS is also beginning to move that capability of scanning overseas through a pilot program we are running in six ports, including a port in the United Kingdom and a port in Pakistan. In addition, we are increasing our footprint overseas in terms of container screening by having about 80 percent of the containers get their initial screening in a foreign port before they even get on a ship.

As it relates to domestic infrastructure, we have issued a proposed new regulation to protect chemical sites; to decrease the standstill time for hazardous rail cargo; to mandate transportation worker identification; and to work with the aviation and maritime sectors to increase security across the board.

In the area of emergency management, we have made the re-engineering of FEMA a priority. We are in the process of completing a reorganization that will be effective on March 31, 2007. In this arena, we have also solidified our partnership with the Department of Defense. We have built real-time information gathering capability that never existed before. We have done a level of planning that is much more detailed than ever envisioned by anybody in a civilian department

dealing with emergencies. All of these things have materially contributed to the security of this country.

• What do you need from Congress in order to continue and expand the good work DHS is doing?

Response: While we have had many successes, there are numerous challenges that still remain. The Department must focus on the greatest risks and be flexible to changing threats, disciplined in our use of resources, and fully committed to building a Department that will meet future challenges, preserve freedom and privacy, and protect the American people. To achieve this, we will place considerable attention over the next two-year period on the following five goals:

- Goal 1: Protect our Nation from Dangerous People
- Goal 2: Protect our Nation from Dangerous Goods
- Goal 3: Protect Critical Infrastructure
- Goal 4: Build a Nimble, Effective Emergency Response System and a Culture of Preparedness
- Goal 5: Strengthen and Unify DHS Operations and Management

Overall, the FY 2008 budget request for the Department of Homeland Security represents an eight percent increase over FY 2007, with a total request of $46.4 billion in funding. The Department's FY 2008 gross discretionary budget is $37.7 billion, an increase of eight percent. Gross discretionary funding does not include funding such as Coast Guard's retirement pay accounts and fees paid for immigration benefits. The Department's FY 2008 net discretionary budget is $34.3 billion, which does not include fee collections such as funding for the Federal Protective Service (ICE), aviation security passenger and carrier fees (TSA), credentialing fees (such as TWIC - TSA), and premium collections (National Flood Insurance Fund, FEMA). It should also be noted that the FY 2008 President's Budget request reflects the Notice of Implementation of the Post–Katrina Emergency Reform Act of 2006 (P.L. 109-295) and of Additional Changes Pursuant to Section 872 of the Homeland Security Act of 2002, provided to Congress on January 18, 2007.

With the support of Congress, the Department has had many successes. We have also learned from our experiences certain things that we could have approached differently to get better results. As we move forward to face the many challenges ahead, those lessons learned will be at the core of our planning.

2. Mr. Secretary, America has almost 200 land ports of entry, and it has been 20 years since we launched a major effort to upgrade infrastructure at those ports. That last effort occurred almost 15 years before September 11, 2001, when former Senator DeConcini and I developed the Southwest Border Improvement Program to improve border infrastructure so that states could better take advantage of commerce and trade opportunities with Mexico. Since September 11, we have placed increasing emphasis on upgrading security for our airports and seaports, but we also need to improve land port security.

• Have you considered what kinds of improvements are necessary at our land ports of entry and how much these upgrades might cost?

Response: We have. Facility and infrastructure needs at our nation's 163 land inspection facilities changed dramatically in the post-9/11 era. Many of our facilities are old: 29 were built in the 1930's and 125 are at least 20 years old. The vast majority were designed to meet needs very different from those of today, and reflect the wear and tear of their years. Large increases in CBP staff to protect our borders and large increases in people, goods, and vehicle traffic in recent years have placed burdens well beyond their intended function and layouts.

CBP's new Capital Investment Plan (CIP) is a systematic and nationwide approach to improving CBP's infrastructure. We developed new land port standards to ensure new construction and refurbished facilities support: (1) modern (and unified) operations and traffic flow concepts, (2) security at and through our ports, and (3) the host of technology systems we now rely upon to operate.

CBP's CIP includes: Strategic Resource Assessment (SRA) site and demographic studies of the conditions and needs of each facility against new standards, a scoring and prioritization method to map directly to mission needs, a five year nationwide investment strategy and annual funding plans, planning database and portfolio management tools, and an annual update process.

• What land port of entry needs do you anticipate in the coming years?

Response: Recent SRA studies have shown a significant gap between our *new mission needs and facility standards* and the *present conditions* at our land port crossings. The four major areas of concern at a majority of facilities are:

- Site Size: Most sites are over capacity, too narrow or have odd boundaries, are located in a right-of-way, and/or are constrained by adjacent land use (i.e., international border, bridgehead or embankment, or connecting roadway infrastructure)
- Site Configuration: Most site layouts constrict traffic flow due to new screening or flow-expediting technologies, lack of pre-primary queue areas, position of buildings and lanes, and/or connecting roadway infrastructure
- Building Size: Most buildings were designed for a different era of inspections and staffing counts, and have no option for simple modification. This has resulted in cramped and unsafe workspaces, limitations to adding technology or functions, and a lack of support space.
- Building Configuration: Most buildings were designed to support the separate operations of several agencies that no longer exist. Internal layout of offices, counters, processing flows, and support spaces are now obsolete and interfere with modern operations and security. They lack critical space adjacencies and secure separation of staff, public, and violator spaces.

• What investments do you foresee DHS making in land port needs in the future?

Response: The funding for land port capital projects at the ninety-seven GSA-owned and at twenty-one GSA-leased land port facilities is provided through the GSA Federal Buildings Fund (FBF). Priority is determined by CBP's CIP. GSA funds and manages the feasibility study, design, and construction costs to bring the facility up to current CBP standards. CBP funds some outfitting of the facilities and reimburses GSA for the amortized cost through rent payments. In some instances, CBP will frontload major construction funding to GSA to eliminate or reduce rent costs. At most of these port facilities CBP funds minor alteration projects, some repairs, overtime utilities, and snow removal.

3. Mr. Secretary, I applaud your efforts to secure our borders. Under your leadership, DHS has initiated the Secure Borders Initiative to take operational control of our borders. Additionally, your FY2006 and FY2007 budgets have called for increased assets for border patrol agents, border security technologies, illegal immigrant detention beds, Immigration and Customs Enforcement personnel, border patrol vehicles and helicopters, and other significant resources.

• Can you tell us a little bit about what the added FY06 resources have meant to DHS and what you expect to do with the FY07 resources you have requested?

Response: The 2006 supplemental and the 2007 DHS appropriation bills will enable DHS to implement an aggressive program to reform our border security and immigration system. Overall, the FY2006 supplemental has helped DHS reach its goal of ending "catch and release" at the border; has expedited the hiring and deployment of more Border Patrol agents; will add miles of additional tactical infrastructure at key junctures along the border; and will provide for tougher enforcement of immigration laws within the United States that includes increased cooperation with our state and local partners and the deployment of more than 3,500 National Guard troops to our southern border in support of DHS, as part of Operation Jump Start.

Operation Jump Start funding in the supplemental also provides an immediate opportunity to get CBP agents out to the front lines. In addition to acting as a force-multiplier through the critical support they provide, these National Guard personnel have allowed significant numbers of Border Patrol Agents to return from administrative duties to front-line patrol.

Expanding the number of Border Patrol agents is one of the core elements of long-term border reform. DHS is committed to the President's strategy of adding 6,000 new agents by the end of 2008, and the FY2006 supplemental provided the initial resources. This supplemental funding will allow the Border Patrol to hire an additional 1,000 Border Patrol Agents and fund related support costs, which will bring the total number of new agents funded in the supplemental and FY 2007 appropriation to 2,500. The Border Patrol will add 6,000 new Agents over the next two years to reach a total level of over 18,300 by the end of 2008.

CBP is buying new vehicles and upgrading facilities in key locations within the Tucson, Yuma, and El Paso sectors. Control of vast stretches of the border requires air support to Border Patrol Agents on the ground. The FY2006 supplemental will enhance that surveillance by purchasing two additional Unmanned Aerial Vehicles (UAVs) and five additional light observation

helicopters. An additional eight light enforcement helicopters will provide direct support to enforcement operations. The supplemental will also allow DHS to spend $250 million in the Yuma and Tucson sectors on vehicle barriers, roads, pedestrian fences, and permanent lighting.

Ensuring the security of our nation's borders requires that we not only secure the actual line of the border, but that we also address the continuum of the violation that occurs when aliens remain illegally in the United States. Finding and deporting alien fugitives, i.e., those aliens who have been ordered removed from the country but who failed to appear for their court date or for removal, is a key element of this enforcement. To that end, DHS is expanding the number of ICE Fugitive Operations Teams. The $20 million in the FY 2006 supplemental will help us accelerate the hiring of more teams in 2007.

The FY2006 supplemental provides funding to expand our current partnerships under section 287(g) of the Immigration and Naturalization Act, which authorizes the Secretary of Homeland Security to enter into written agreement to delegate limited immigration enforcement authority to state and local officers.

The FY2007 Department of Homeland Security appropriation will provided the resources to acquire more technology and physical infrastructure along the border as part of SBInet.. This bill will include funding for an additional 1,500 Border Patrol agents, 6,700 detention beds and $1.2 billion for border fencing, vehicle barriers, technology and tactical infrastructure.

The mix of the FY2006 supplemental and the FY2007 appropriation investments will enable the Department to make substantial progress toward preventing terrorists and others from exploiting our borders and provides flexibility for smart deployment of physical infrastructure that needs to be built along the southwest border. All these efforts will allow DHS to make great strides towards securing all U.S. borders.

• What border security needs do you anticipate in the coming years?

Response: Ensuring the security of our nation's borders requires that we not only secure the actual line of the border, but that we also address the continuum of the activity that leads to border security violations outside and within our borders. Implementation of the Western Hemisphere Travel Initiative (WHTI) represents a critical change in our ability to secure our ports of entry operations and ensure that individuals can no longer merely claim U.S. citizenship to enter by land and sea. CBP officers will have the tools they need to increase security, improve their targeting capabilities, and facilitate legitimate trade and travel. Clearly, in hardening our borders, we must also address violations that occur within our borders. We must commit to providing businesses with additional lawful ways to hire labor, and to address the status of the estimated 12 million immigrants we believe are currently in our country illegally. A guest or temporary worker program that will allow for lawful employment and entry of foreign workers will afford American businesses access to workers without breaking the law.

Additionally, we must foster a culture and build tools to support voluntary compliance with immigration laws. DHS must be able to address both compliance and enforcement programs to enable a more effective response to border security and immigration vulnerabilities.

4. Mr. Secretary, your Department has a new office tasked with deploying radiation detection technologies and systems to detect attempts to smuggle nuclear materials or weapons into the U.S. As such, the Domestic Nuclear Detention Office is likely to play a critical role in testing and evaluating current and next generation technologies to assure that DHS agencies have the most effective and accurate tools possible.

• In the coming years, how will you develop and support the nuclear facilities and infrastructure needed to test and evaluate evolving technologies, missions, and operational concepts?

Response: The DNDO relies heavily on the ability to obtain high fidelity, defendable test data in support of development, acquisition, and deployment decisions. The DNDO has made a commitment to fully characterize all technologies prior to large-scale acquisition decisions, to ensure that DNDO understands potential performance improvements and liabilities.

The construction at the Nevada Test Site (NTS) of the DNDO Radiological and Nuclear Countermeasures Test and Evaluation Complex (Rad/NucCTEC), scheduled for completion in FY 2007, will offer the opportunity for high-fidelity test and evaluation. The Rad/NucCTEC will be authorized to handle special nuclear material (SNM) for the purpose of testing commercially-available and newly-developed technologies against actual samples of these materials which provide the greatest threat to the Nation for use in a nuclear attack. Prior to the construction of this facility, no location existed that allowed access to these quantities of materials while maintaining the flexibility to place these materials into relevant threat scenarios and cargo configurations.

• Our national weapons labs have done some work with DNDO. What role do you see the labs playing in the future?

Response: The DNDO recognizes that the national weapons laboratories have long been one of the Nation's preeminent sources of critical nuclear expertise. That expertise, along with the expertise found in other National and Federal Labs, academia, and industry, is vital in developing technologies to mitigate the threat of radiological and nuclear terrorism.

The largest role that the National Labs will have within the DNDO is within the transformational research and development program that seeks advanced, novel solutions to develop significantly more effective, capable, and operable nuclear and radiological countermeasures. In December 2005, the DNDO released a call for proposals (CFP), soliciting nuclear detection exploratory research proposals from the National Labs. The DNDO received over 150 proposals (of which nearly 50 were selected) and anticipates awarding over $35 million for these research efforts in FY 2006.

Additionally, the DNDO relies on the nuclear expertise within the National Labs to support efforts across the office. For instance, National Labs provide analysis towards the development of the global nuclear detection architecture, deployment support to the Radiation Portal Monitor (RPM) program, testing support at NTS, and operational support through the Nuclear Assessment Program (NAP) and the Technical Reachback (TRB) program. In support of the new forensics mission that DNDO will undertake in FY 2007, the National Labs will play an integral role in the development of forensics signatures, databases, and analysis techniques to discriminate nuclear material supply origins. Also, the DNDO National Technical Nuclear Forensics Center (NTNFC) its associated data base will be coordinated and support the Nuclear Materials Information Program (NMIP) that is managed by the Department of Energy (DOE). The DNDO intends to continue to rely heavily on this expertise as the global architecture continues to evolve and mature.

• How do you foresee DNDO interacting with the Department of Energy's efforts in the same areas?

Response: The DNDO interacts with DOE in relation to research and development as well as deployment planning. DOE, as the agency with the most historical experience in nuclear countermeasures, provides detailees into every DNDO office.

The DNDO (particularly the transformational research and development program) works closely with the National Nuclear Security Administration (NNSA) Office of Nonproliferation Research and Development (NA-22). Staff from both NA-22 and DNDO served on each others' proposal review panels, in part to ensure that duplication of funding is avoided. In addition, this interaction helped ensure that DNDO transformational R&D programs are well coordinated with those of NA-22 (which focused on foundational science for advanced detectors and materials), enabling the U.S. Government to best utilize the expertise of the National Labs. DHS, through the DNDO, also voluntarily participates in the Counterproliferation Program Review Committee (CPRC), co-chaired by the Department of Defense (DoD) and DOE with members from DNDO, the Intelligence Community, State Department, and others, which provides a yearly report to Congress and works to ensure that technology development in the R&D area is fully coordinated. It should be noted that DNDO and DHS are not formal members of the CPRC and representation is not required by the Defense Authorization Act that governs the CPRC reports.

Additionally, in FY 2005, as part of the overall R&D coordination process, the DNDO supported the Domestic Nuclear Defense (DND) R&D Working Group (chartered by the Homeland Security Council and the National Security Council) to develop a coordinated, interagency R&D roadmap that would enhance the breadth of domestic nuclear defense efforts to ensure a secure nation. The scope of the DND R&D Working Group covered the interagency coordination of R&D strategies for domestic nuclear defense, the identification and filling of critical technology gaps, efforts to develop and sustain critical capabilities through appropriate investments in foundational sciences and research, interagency funding for necessary science and technology, and collaboration and exchange of vital R&D information. The DNDO co-chaired the working group on interdiction research and development.

DOE employees have been assigned to provide support to overseas deployment planning and logistics—implementation missions that remain with DOE and NNSA. The DNDO, through its Joint Analysis Center (JAC), is currently working with DOE and other partners to help secure agreements for more timely and uniform information sharing from overseas screening operations. The DNDO is also now working with the NNSA Office of International Material Protection and Cooperation (NA-25) to acquire ASP systems for deployment through the Megaports Initiative, further enhancing the broader U.S. strategy to scan incoming cargo before it reaches our borders. Additionally, detailee staff are developing Federal reachback programs that can draw upon expertise within the National Labs, as needed, to provide technical support to resolve alarms generated in the field.

Questions from Senator Joseph I. Lieberman

1. Despite the growing concerns about security threats to this country, the Urban Area Security Initiative, the State Homeland Security Grant Program, and the Law Enforcement Terrorism Protection Program, have shrunk dramatically over the last three years, dropping in half from nearly $3 billion in FY04 to less than $1.5 billion in the President's budget for FY07. A 2004 survey by the U.S. Conference of Mayors found that 89% of cities reported that limited funding was their chief obstacle to communications interoperability; according to the National Task Force on Interoperability, replacing basic radio systems for a single public safety agency at the state level can cost between $100 million and $300 million. Will you seek to reverse this trend over the next five years and increase homeland security funding for state and locals?

Response: Homeland security is a shared mission and thus a shared responsibility between the federal government and our state and local partners. The federal government cannot be expected to bear all homeland security costs. Instead, the Department expects that States and localities will devote significant funds to enhance their security and thereby help to improve the Nation's level of preparedness.

Additional funding for State and local interoperable communications funding was authorized by Public Law. 109-171, the Deficit Reduction Act of 2005, and is contingent upon auction of public radio spectrum frequency licenses. Up to $1 billion through Fiscal Year 2010 may become available to support communications interoperability and will be subject to State and local financial matching requirements. DHS looks forward to continuing to work with Congress to determine the most appropriate way to allocate scarce resources in a way that balances risk with need.

2. Despite the spread of IED attacks in Europe and the Middle and Near East, the Chief of the Bombing Prevention Unit of DHS' Risk Management Division informed staff that no state or local bomb squads, with the exception of New York City's, possess electronic countermeasures for explosives. Although the federal government possesses such technology, it has not distributed it to local bomb squads in the United States. Will DHS share this technology with bomb squads in other cities through a technology transfer, and will DHS make this technology

something state and local governments could apply for through homeland security grant funding to them?

Response: DHS' Office for Bombing Prevention (OBP) within the Office of Infrastructure Protection coordinates national and intergovernmental bombing prevention efforts and conducts requirements, capabilities and gap analyses. OBP will analyze activities and capabilities such as electronic counter measures (ECM) as part of developing the National Strategy for Bombing Prevention.

Currently, the FBI and the Department of Defense's Technical Support Working Group (TSWG) are currently implementing a pilot program to test, select and deploy ECM equipment for State and Local bomb squads. The limited pilot program has very recently outfitted New York and Seattle and is set for other deliveries in FY07. The pilot, which is being conducted with DHS participation, will deploy ECM equipment to 10 of the Nation's 460+ bomb squads. Central to this effort is determining deployment and equipment challenges at the state and local level in varying environments for both vehicle-mounted and man-carried ("walk down") ECM.

Training and certification for the operation of this equipment, as well as licensing with the FCC and National Telecommunications and Information Agency (NTIA), is being conducted by the FBI (equipment will be operated by State and Local squads under an FBI license).

Using the knowledge gained from the pilot, as well as lessons learned from the efforts of the Joint IED Defeat Organization, DHS can assist in several ways to ensure that State and Local bomb squads achieve increased capabilities. This necessary training and outfitting can be accomplished through mobile training teams and grant funding. The DHS Office for Bombing Prevention (OBP) is currently working to implement changes to the current FY07 grant guidance and Authorized Equipment List to address several bombing prevention capability gaps that include ECM. Currently, costs for the equipment are estimated at $90,000 per ECM unit.

Any effort to improve ECM capabilities should be conducted in partnership with FBI to ensure squads are trained, equipped, certified, and licensed consistently. Deployment of multiple or incompatible ECM equipment would cause negative results. Further, use of ECM without a license is a violation of Federal (as well as some State) statutes.

DHS and FBI are currently working to determine the process for developing ECM standards through organizations such as the National Institute of Standards and Technology (NIST). Such standards are essential to ensure the effectiveness of ECM equipment purchased through a grant program.

Additionally, fixed ECM for high-risk Tier I and II critical infrastructure sites are necessary to achieve optimal protective capacity as a threat-initiated action. OBP is conducting a national analysis to determine the best course of action to address such gaps in capability.

3. In their testimony, witnesses from the second panel criticized the federal government for its failure to provide state and local law enforcement officers with adequate information. The Markle Foundation and DC Police Chief Ramsey have also criticized the federal government's failure to mobilize information for security purposes. Enhancing the sharing of information benefits everyone – the police on the street benefit from the best intelligence the federal government has to offer, and in turn the federal government could learn mountains from the same police on the street. Richard Falkenrath of the New York City Police Department's Counter Terrorism Program argues that the federal government's information-network should include his force and other local police forces as full-fledged members, as opposed to the federal government selectively piping bits and pieces of information from that network to local law enforcement. Does DHS intend to more fully incorporate the NYPD's Counter Terrorism force and other major law enforcement units in other cities and states in the federal government's Information Sharing Environment, as the Intelligence Reform and Terrorist Prevention Act envisioned, or will the Department simply continue to provide information to local law enforcement only on a selective and ad hoc basis?

Response: DHS is incorporating major law enforcement units in other cities and states, in the information sharing environment, through I&A's State and Local Fusion Center support program. This program makes the Intelligence Community more accessible to our state and local partners. These centers are established using the *Fusion Center Guidelines for Establishing and Operating Fusion Centers at the Local, State, and Federal levels*, which both DHS and the Department of Justice endorsed.

DHS is currently allocating personnel, resources, and systems to these fusion centers. In every fusion center where a DHS analyst is stationed, we will connect that officer to the SECRET-collateral HSDN, which in turn connects to the Intelligence Community's SECRET-level network. In addition, we will provide certain state and local officials with HSDN access. For example, NYPD already has two HSDN installations in the New York fusion center and embedded NYPD officers are nominated for HSDN passwords. This will give NYPD access to the Intelligence Community's products, as well as providing a SECRET-level system to allow NYPD officers to collaborate with the Community's intelligence analysts. We started this process this year and will have at least 35 fusion centers staffed by FY 2008. Our goal is to enable NYPD, and agencies in other key states and cities within the information sharing environment, using DHS personnel, resources, and systems in the field. Through these efforts, state and local law enforcement will be integrated into all aspects of the federal government's information sharing environment, as envisioned by the Intelligence Reform and Terrorist Prevention Act of 2004.

4. In your testimony you noted that DHS has provided $2.1 billion to states since 2003 for interoperable communications equipment, planning and training. Yet the estimated cost for achieving interoperability nationwide is at least $40 billion, according to one estimate from the SAFECOM office within DHS. You stated to our Committee that you would "hesitate to dedicate a huge amount of money up front, without the input of the localities themselves to make a determination of what they feel they need and how far they've come and what their remaining

gaps are." Many States and localities, though, already have identified investments that can help achieve interoperability. For example, just this week the City of New York announced a $500 million contract to build a wireless broadband public safety network. Why, when the need is so great and so clear, will you not support a dedicated grant program for interoperability?

Response: The Department supports interoperability grants by working closely with states and localities to facilitate smart interoperability investments that will build future capabilities. DHS believes that state and local emergency response agencies are in the best position to identify their areas of greatest need. In the instances when states and localities have already identified investments that can help achieve interoperability, they can use their Homeland Security Grant Program (HSGP) funding to support those investments. SAFECOM, a communications program of the Office of Emergency Communications (OEC) works closely with Federal grant programs that provide funding for interoperable communications to the emergency response community (Elements of SAFECOM were recently transferred from the Office for Interoperability and Compatibility (OIC) within the Science and Technology Directorate. Responsibilities for research, development, testing & evaluation and standards will remain within OIC). For example, SAFECOM developed the "Recommended Federal Grant Guidance" to maximize the grant dollars available for emergency response communications and interoperability by providing recommended criteria for grant applicants and principles and guidelines for interoperability activities. The guidance provides recommended criteria for who is eligible for Federal grants, purposes for which grant funds can be used, and guidelines for implementing a wireless communications system. SAFECOM first developed the grant guidance in 2003. Since that time, the grant guidance has been included in the Department of Justice's Community Oriented Policing Services grants as well as those of DHS Office of Grants and Training (G&T). The grant guidance was also included in the Federal Emergency Management Agency's (FEMA) interoperable grants in FY 2003, the only year FEMA distributed such grants. SAFECOM is also working with the Department of Commerce's National Telecommunications and Information Administration (NTIA) and G&T to incorporate SAFECOM's grant guidance into NTIA's new interoperable communications grants.

There are also instances where states and localities have not comprehensively identified needs. To address this issue, DHS has taken steps to assist the emergency response community in identifying areas of need in order to target and maximize the use of grant funding. For example, DHS is in the process of measuring the interoperable communications capability in 75 major urban/metropolitan areas. This initiative builds on RapidCom, an effort led by SAFECOM and G&T in FY 2004 that focused on achieving tactical-level emergency interoperable communications in ten major urban areas. The FY 2005 Homeland Security Grant Program (HSGP) required 75 major urban/metropolitan areas to develop a Tactical Interoperable Communications Plan (TICP). The TICPs were due on May 1, 2006 and all 75 have been submitted and reviewed. Each TICP then has to be tested and validated through an exercise which must be completed by October 30, 2006. Following the exercise, the sites will receive an after-action report and improvement plan which will lead to the development of a scorecard based on the SAFECOM Interoperability Continuum. The Department is also requiring each state to develop a Statewide Communications Interoperability Plan. These plans are due at the

end of 2007. All of this information will help states and urban/metropolitan areas determine their current communications capability and make smart investments in the future to improve this capability.

5. In remarks you delivered at Georgetown University on September 8, you stated that DHS has "initiated" a baseline survey to assess interoperability needs across the country. Your written testimony before our Committee states that the survey has been "completed." But in your oral testimony to the Committee, you stated that DHS is "planning by the end of the year to have done a careful study...." DHS staff first briefed our Committee on the initiation of the baseline survey roughly 18 months ago.

• What is the status of the survey?

Response: The S&T Directorate administered the National Interoperability Baseline Survey on voice communications to approximately 22,400 randomly selected emergency response organizations during May-July 2006. The survey and the Initial Results Report were completed in August of 2006. The S&T Directorate is conducting further in-depth statistical analysis that will be published as part of the Final Results Report, which will be available before the end of the calendar year. These results will provide an accurate picture of the state of interoperability among law enforcement, fire, and emergency medical service responders across the Nation.

• Why has completion of the survey taken so long?

Response: Numerous steps are necessary for the creation of a survey of this breadth and magnitude. First, in accordance with its practitioner driven approach, SAFECOM, then a program of OIC, recognized that input from the emergency response community was essential to the development of an effective survey—one that could produce an accurate picture of the state of interoperability across the Nation. SAFECOM conducted four focus groups with emergency response representatives across the Nation to inform the measurement tool and language of the survey. The time required to organize, develop, and execute these focus groups was significant. Based on the data gathered in these focus groups, the survey was refined multiple times. The final survey was then reviewed and validated by another group of emergency response practitioners. Upon validation, SAFECOM piloted the survey with a group of practitioners to gain further input on the content, format, and usability of the survey. Second, SAFECOM conducted 36 site visits in nine regional areas in order to gain a better understanding of the results derived from the survey responses. Finally, time is needed to fully analyze the responses.

• When will DHS complete this baseline assessment, which is critical to providing us a road map for finding solutions for interoperability?

Response: The Initial Results Report was completed in August of 2006. Further in-depth statistical analysis is being conducted and will be included in the Final Results Report, which will be available by the end of the calendar year.

6. Aside from the baseline survey, what do you plan on doing to make sure that DHS comes up with a long-term strategic plan for achieving interoperability and to make sure that DHS, at a high level, is aggressive in its outreach to State and local governments to help them solve interoperability problems?

Response: In addition to finalizing results of the National Interoperability Baseline Survey, SAFECOM is pursuing a long-term strategy for strengthening interoperability. This strategy incorporates a comprehensive approach to communications interoperability, which includes critical success factors to interoperability such as governance, standard operating procedures, training/exercises, and usage. In addition to this long-term strategy, SAFECOM is implementing, a short-term strategy to assist the emergency response community in improving interoperability in the near term.

SAFECOM supports this strategy by providing tools and resources that assist the emergency response community in implementing a comprehensive solution to interoperability. Below are a few highlights of ways that SAFECOM has assisted the emergency response community in the near term:

- Published the Statewide Communications Interoperability Planning (SCIP) Methodology—step-by-step planning guide for developing a locally driven statewide strategic plan, setting the foundation for interoperable communications;
- Conducted the Regional Communications Interoperability Pilots (RCIPs)—initiatives coordinated on the ground to assist implementation of statewide planning processes which will result in models and tools for all fifty states;
- Led RapidCom 1—initiatives in the top ten high-threat urban areas to establish emergency communications at the command level within one hour of a major incident; provided policy guidance, facilitated table top exercises, and supported governance bodies;
- Assisted in RapidCom 2—technical assistance provided by the Office of Grants and Training to assist Urban Area Security Initiative sites in developing and exercising on Tactical Interoperable Communications Plans;
- Published Public Safety Architecture Framework (PSAF) Volumes I and II—documents that help emergency response agencies map system requirements and identify system gaps;
- Published the Statement of Requirements (SoR) Volume I, v1.0 and v1.1—documents that provide specifications to manufacturers and enables them to build equipment that meets emergency responders' communications needs;
- Conducted the Roundtable on Public Safety Interoperability and Voice over Internet Protocol (VoIP) along with the National Institute for Standards and Technology (NIST) – meeting of public safety and industry representatives to discuss VoIP's role in communications interoperability for the emergency response community;
- Provided continued support of the acceleration of the Project 25 (P25) suite of standards, which will help produce equipment that is interoperable and compatible regardless of manufacturer; and

- Provided common grant guidance to Federal programs—provided recommended criteria to Federal grant programs that offer funding to State and local agencies for communications interoperability; the guidance fosters cross-jurisdictional and multi-disciplinary interoperability planning and funding.

The following is a list of some of the tools and resources that will soon be available to the emergency response community to assist in improving interoperability:

- Guide for a Memorandum of Understanding (MOU) – tool that provides information on creating a framework for mutual accountability among multiple jurisdictions;
- Guide for Standard Operating Procedures (SOP) Version 1 – tool that provides instructions to assist emergency responders in creating effective SOPs;
- Request for Proposal (RFP) Guidebook – guide to assist practitioners with the RFP development process that will help maximize resources and inform purchasing decisions; and
- Guide to Improving Interoperability through Shared Channels – guide to help state and local interoperability coordinators understand the steps needed to implement one type of interoperability solution, using existing resources.

7. As Hurricane Katrina showed us, you cannot have interoperability unless you have basic operability. What is DHS doing to make sure that in the event of a catastrophic loss of local and regional communications, the federal government is ready to assist in providing back-up communications capabilities to ensure basic operability for first responder communications?

Response: In response to previous disasters, FEMA has occasionally provided limited communications support to first responders when their systems have been damaged or otherwise inoperable. However, none of those occasions was as extensive as needed to overcome losses due to the catastrophic damage of Katrina.

DHS realizes we must be able to provide more extensive communications support for first responders when conditions demand. FEMA is currently examining shortfalls in our systems and resources that could be used to augment or backfill local responders' communications systems if and when needed. Included in this requirement are radio, phone, satellite, and information systems. In addition, we recognize the need to bring in temporary 911 centers as required.

In this evaluation we will be examining alternatives to purchasing and warehousing backfill equipment such as contingency contracts for temporary use of commercial standby systems, similar to what we have done in the past for landline telephone switches. FEMA is also examining options to augment its ability to more rapidly assess damage and develop alternative communications solutions immediately after a disaster occurs. In some cases, it may be quicker to assist the first responders to make repairs on existing damaged systems than to bring in and distribute alternative systems. As has been demonstrated in the Gulf Coast communications plans developed for Louisiana, Mississippi, and Alabama this year, we can and will improve our understanding of state and local first responder communications systems and help them identify

remedial actions they could take before a disaster in order to mitigate damage, as well as plan for outages and identify readily available alternatives.

8. DHS' "can do, will do" attitude toward aviation security should be applied to mass transit and passenger rail security, especially in light of the attacks in Madrid, London, and India. This is an enormous concern. For example, in Connecticut, 110,000 people use the New Haven MTA line every day. Yet the Department's own press release from last week stated that DHS has spent $375 million on transit security. This is compared to the over $6 billion the American Public Transportation Association says is necessary to secure our mass transit systems, and when compared to the more than $18 billion spent by DHS on aviation security. The President's latest budget did not dedicate funds to transit security. By leaving mass transit less secure, DHS places an even greater strain on our first responders. Will DHS ask the Administration to dedicate sufficient funding in next year's budget to the protection of the nation's mass transit and passenger rail systems?

Response: DHS has consistently stated that mass transit security and passenger rail security are a shared responsibility among a variety of stakeholders, including state, local, and Federal agencies, and private owners and operators. Since 9/11, the Federal Government has dedicated an estimated $900 million to transit security. This figure encompasses grant programs administered by the Department of Transportation (DOT), Federal Transit Administration (FTA), DHS, and the Transportation Security Administration (TSA), as well as part of TSA's annual appropriation for surface transportation security (including funds earmarked for inspectors and canines). In FY2006, DHS dedicated approximately $143 million to passenger rail and rail transit and bus transit security.

Additionally, FTA annually awards more than $3.5 billion in capital improvement grants. These funds may be used for capital security enhancement. Under the Safe, Affordable, Flexible, Efficient Transportation Equity Act – A Legacy for Users, up to two percent of these grants may be dedicated to security training and exercises.

The $900 million cited does not reflect the value of supporting services the Federal government provides to transit security through funding of broader security efforts, such as the Transportation Security Operations Center, the Transportation Security Intelligence Service, and DOT's Crisis Management Center. These and other programs contribute to accomplishing the surface transportation security mission. The intelligence and information-sharing and alert capabilities maintained through these processes are key components of the layered approach to transit and rail security.

Clearly, the majority of Federal spending on transportation security has gone to aviation. These expenditures cover the costs associated with maintaining a force of Transportation Security Officers – screeners – to operate security checkpoints in airports. This model does not apply in transit. The model's openness and accessibility, essential to efficient operations in getting the huge volume of passengers to their destination, precludes this sort of point defense. The Federal Government has used a risk management approach to focus its spending on transit security

through grant programs, deployment of Surface Transportation Security Inspectors and explosives detection canine teams, joint exercises to supplement security in transit systems with TSA resources, technology pilots, and other targeted initiatives. The fundamentals include:

- Protection of underwater/underground assets and systems that are at high risk and, if seriously damaged, would have high consequences;
- Protection of other high risk/high consequence assets that have been identified through system-wide risk assessments;
- Use of visible, unpredictable deterrence;
- Targeted counter-terrorism training for key front-line staff;
- Emergency preparedness drills and exercises;
- Public awareness and preparedness campaigns; and
- VIPR Teams.

9. DHS informed our staff that it would not be disbursing transit security grant funds to recipients until the end of September, the last day of the fiscal year. This money comes much too late, at great risk.

• Will you commit DHS to disbursing these funds earlier in the fiscal year, next year?

Response: During the September 25, 2006 announcement of the FY 2006 transit security grant funds, the Department committed to announcing grant awards earlier in the next fiscal year. In addition, the FY 2007 DHS Appropriations bill included mandatory deadlines by which the guidance must be released.

• What will you do to expedite the disbursement of these funds?

Response: DHS plans to release the FY 2007 application kit in accordance with statutory deadlines.

10. As you know, the Senate recently passed major port security legislation. The bill addresses both major components of U.S. port security – the physical security of domestic ports, and the security of the international supply chain and cargo containers, which move 95% of commerce coming into the U.S. Will you seek the funding necessary to make sure that the goals for port security in HR. 4954 become a reality?

Response: The Department will seek the necessary funding to ensure we meet the port security goals as set in H.R. 4954. This will include supporting vital programs, such as the Customs-Trade Partnership Against Terrorism, the Container Security Initiative, deployment of radiation and imaging technology to our ports of entry, and the implementation of the Pilot Integrated

Scanning System. The Department believes that these programs will provide added value to national security by improving maritime and cargo security.

11. For more than two years, DHS has been working on the Transportation Worker ID Credential (TWIC) program, which is designed to help improve the physical security of our ports by controlling access of individuals to the secure area of the port. DHS has announced that it intends to issue TWIC ID cards to 750,000 port workers, even though the machines that read these cards have not been approved through a rulemaking. DHS has also announced that ports will not be required to purchase or install biometric card readers at port entrances during Phase I of the TWIC implementation.

• What good are these biometric cards, if there are no machines to read them?

Response: The proposed rule for the Transportation Worker Identification Credential (TWIC) would increase security at vessels, facilities, and Outer Continental Shelf (OCS) facilities and mitigate the threat posed by individuals with unknown backgrounds accessing vessels and facilities. Once implemented, this rule would:

(1) Reduce the number of high-risk individuals having unescorted access to secure areas of vessels, facilities, and OCS facilities through robust security threat assessments that include criminal history records checks, immigration status checks, and checks for ties to terrorism;

(2) Issue a secure, biometric credential to the individual that is linked to the security threat assessment; and

(3) Require TWICs for all individuals with unescorted access to secure areas.

Based on comments received from all sources, the Department has proposed to bifurcate the rule. To address concerns about the adequacy of current reader technology, TSA and the Coast Guard will not require facility and vessel owner operators to purchase, install, and maintain card readers in this rule. We will address this requirement at a later date and provide all interested parties ample opportunity to comment on any new proposals. As part of this effort, TSA and the Coast Guard are working with the Ports of Los Angeles and Long Beach, which have received a $12 million Port Security Grant, to field test the use of card readers for access control. This field test is examining cost concerns with respect to card readers and evaluating the issue of reliability of the readers in a commercial and/or marine environment.

The TWIC will be incorporated into existing security measures as outlined in the applicable vessel and facility security plans. In practice:

- an owner or operator can verify the TWIC by having an individual match the photo on the credential to the individual presenting the credential;
- An owner or operator can confirm the validity of the TWIC, and the risk posed by the individual accessing the secure area, by verifying the TWIC's expiration and checking the various security features on the card for evidence of tampering; and

- The U.S. Coast Guard (USCG) will perform checks, either randomly or for cause, using hand-held biometric smart card readers, as part of its normal port and vessel compliance inspections.

These measures should increase security across the maritime transportation sector. Furthermore, owners or operators that have electronic access control systems will be capable of achieving higher security levels if they choose to update those systems to recognize the TWIC.

Enrollments will be phased in for the initial estimated population of 750,000 affected port workers and merchant mariners over an 18 month implementation period in coordination with the local Coast Guard Captains of the Port. The rollout plan, including schedule and location of the initial ports, will be finalized once the enrollment contractor has been selected. TWIC compliance will be phased in by Captain of the Port Zone based on the enrollment rollout plan with national compliance expected 18 months after the effective date of the final rule.

• Why is the Department issuing ID cards to 750,000 people, if the cards might change? This could mean the reprinting of 750,000 cards, coming at significant expense to the taxpayers.

Response: We are making every effort to prevent the need for reprinting; however technology is ever evolving. A major focus is being placed on backward compatibility for TWIC reader technology.

DHS will issue Transportation Worker Identification Credentials (TWIC) to maritime workers requiring secure access to port facilities and vessels. Today, port facility and vessel owners and operators do not have the benefit of a standard, uniform, and secure credential. Port workers do not routinely have security threat assessments to identify criminal histories or links to terrorism. Conducting security threat assessments on all individuals with access to secure areas is the first step in improving security at the nation's ports. By issuing the TWIC, DHS is providing owners and operators with an important tool to identify individuals who have successfully completed a security threat assessment.

DHS has based the smart card technology for TWIC on the new standard for identity cards for all Federal government employees and contractors, Federal Information Processing Standard (FIPS) 201-1. This standard was driven from Homeland Security Presidential Directive – 12. In the first phase of TWIC, FIPS 201-1 smart cards will be issued to applicants.

DHS plans to address requirements for readers in a forthcoming rulemaking and will conduct field tests of reader technology to identify best practices for TWIC implementation and to obtain data on biometric readers.

• How much would it cost to reprint these cards?

Response: We are making every effort to prevent the need for reprinting.

12. Five years ago, the 9/11 terrorist attacks took us by surprise. A year ago, Hurricane Katrina exposed a flawed response by the federal government to a national catastrophe. Hurricane Katrina put us all on notice that we still have a long way to go to ensure an effective federal response to the large scale catastrophic events whether they are caused by terrorism or natural disasters. Unfortunately, concerns remain about the Department's state of preparedness for a catastrophe. For example, a recent GAO report found that DHS still hasn't finalized the Supplement to the Catastrophic Incident Annex, which, according to GAO, means federal agencies with responsibilities under the Supplement "cannot complete the implementation plans and agreements needed to make the annex and supplement fully operational."

• Why has the Supplement not been finalized? Have DHS components or other federal agencies raised concerns to you about the draft Supplement? If so, what are they, and what is DHS doing to address them?

Response: DHS officially signed off on the NRP-CIS and approved its release on August 15, 2006. The Catastrophic Incident Supplement (CIS) has been finalized and was rapidly distributed within DHS and to each Federal supporting department via protected electronic means on August 16. Further distribution by paper copy of a document designated as For Official Use Only (FOUO) will occur by mid-October. The CIS is also available on-line to Federal, State, local and tribal authorities that have access to the password protected Homeland Security Information Network (HSIN) where it was posted on September 13 to the Emergency Management, Federal Operations, Catastrophic Planning and Law Enforcement portals.

The CIS was developed and prepared by a Federal Agency Task Force composed of the following government agencies/organizations: Department of Transportation, Department of Defense, Department of Justice, Department of Energy, Department of Interior, US Department of Agriculture, Health and Human Services, Transportation Security Administration, US Coast Guard, Environmental Protection Agency, American Red Cross, US Forest Service, US Army Corp of Engineers, Occupational Safety and Health Administration, Tennessee Valley Authority, National Oceanic and Atmospheric Administration, and the National Communication System. Not all NRP signatory Departments and Agencies participated in the development of the CIS as it only focused on the following key areas: mass care, search and rescue, decontamination, public health and medical support, medical equipment and supplies, victim and fatality management and transportation and public information. Agencies with expertise in the areas identified were selected to participate in its development.

The NRP-CIS was approved by all Task Force members and also approved by all DTRIM agencies, except DoD on May 27, 2005. DoD concurred when National Disaster Medical System concerns were resolved. A major review and rewrite of the National Response Plan, including the CIS, will soon commence and every original signatory of the National Response Plan, along with identified State, local, tribal and private sector representatives will participate in its review.

• When will the Supplement be finalized?

Response: The CIS was approved on August 15, 2006, and was distributed through the Homeland Security Council to the primary DHS offices involved in its implementation on August 16, 2006. The CIS also is available on-line to DHS offices through the password protected Homeland Security Information Network (HSIN). The information was posted on September 13 to the Emergency Management portal, the Federal Operations portal, the Catastrophic Planning portal, and the Law Enforcement portal. When it was posted on HSIN, Federal, State and local officials who have been given access to the specified portals on that system had immediate electronic access.

13. One of DHS' primary responsibilities under Emergency Support Function 5 (ESF-5) of the National Response Plan (NRP) is to monitor the operational readiness of all federal agencies to respond to large-scale catastrophic incident. However, a recent GAO report found that "currently, there is little available information on the operational readiness of many of the reforms and actions DHS has announced in recent months."

• Under ESF-5 of the NRP, has DHS reviewed the current operational response plans of the departments or federal agencies with primary missions under the National Response Plan to ensure that they are adequate for catastrophic incidents?

Response: The National Response Plan (NRP) establishes a single, comprehensive approach to domestic incident management to prevent, prepare for, respond to, and recover from terrorist attacks, major disasters, and other emergencies. The NRP is applicable to all Federal departments and agencies that have primary jurisdiction for or participate in operations requiring a coordinated Federal response.

Under the NRP, Emergency Support Function (ESF) Annexes provide detailed descriptions of the mission, policies, structure, and responsibilities of Federal agencies for coordinating resource and programmatic support to a State or other Federal agencies during an incident. ESFs were established as an effective mechanism to group capabilities and resources into the functions that are most likely needed during actual or potential incidents where coordinated Federal response is required.

All of the ESFs have developed and submitted NRP ESF Annex Standard Operating Procedures (ESF SOPs) to be included in the revised NRP. The majority of the ESFs will continue to refine and validate their SOPs and practices based on situation-specific information obtained immediately before the incident or during the initial post-incident damage and need assessments.

The FEMA Response Division has conducted one-on-one meetings with the ESF Agency/Department Coordinators to ensure that the ESFs are prepared to execute their ESF SOPs and commence operations consistent with the NRP in preparing for, responding to, and recovering from an incident. FEMA also coordinates with ESF partners in developing strategic, time-sequenced plans of preparedness, response actions, and decision making points. The objective of these ongoing one-on-one meetings is to bolster operational readiness and ensure

that the ESFs have the capability to maintain comprehensive situational awareness, proper coordination, and resource/action tracking visibility during an incident.

A review and revision of the NRP will be co-chaired by FEMA and DHS Preparedness with participation from all levels of stakeholders (Federal, State, local, tribal, private sector and NGOs). The review will consider lessons learned and best practices identified during exercises and disaster responses and must reflect the views and understanding of all emergency management partners across the country. As part of this review, all of the signatories to the NRP will have an opportunity to further review, comment on, and adjust the various components of the Plan.

• Have all the federal agencies with missions under the National Response Plan made the investments, done the training and conducted the exercises that you believe are necessary? If not, which agencies have yet to make the necessary improvements?

Response: A major review of the NRP will be initiated in October and conclude in the Fall of 2007 that will include participation from all NRP signatory agencies. During the review, key issues will be identified and addressed. The review will also result in the development of training materials in a variety of formats and development of a series of exercises to test the new plan. Preparedness in general continues to be a work in progress for most federal agencies. Agencies such as the Environmental Protection Agency and the U.S. Coast Guard are much further along due to their ongoing responsibilities under the National Contingency Plan. As the "National Exercise Program" continues to mature, more agencies will have the opportunity to conduct training and exercises in an interagency model.

• Are there any federal agencies with primary or support missions under the NRP whose shortcomings in terms of the equipment, personnel, technology, operational procedures or training are sufficiently serious that they would jeopardize their missions under the NRP in the event of another catastrophic terrorist attack or natural disaster? If so, which agencies?

Response: DHS initiated a major review of key areas identified as weaknesses in after action reports associated with Hurricanes Katrina and Rita. Accordingly, DHS initiated a major effort across the Federal response and recovery community to address contracting shortfalls, resource limitations, equipment problems, functional alignments, and reporting structure failures. As a result of this effort, the federal government is far better prepared to deal with a future catastrophic event.

14. DHS was established to forge a new security capability built of some existing programs and some new ones, but all brought together into a dynamic new structure focused on meeting a new threat to our country. Although there have been some efforts to integrate component agencies – for example, cross training immigration and customs border agents for the "One Face at the Border" program – too often the Department's many parts continue to operate as independent players without a unifying vision. This was evident with tragic results in Katrina, where information and assets were not shared freely and effectively. It is evident in the chaos besetting

S&T, which was meant to provide leadership and priorities for the Federal government's homeland security R&D but instead has lacked the funds and guidance to even run its own affairs.

• What is your view of the Department's cohesiveness? What steps are you taking to bring greater unity to its work?

Response: Recent challenges such as Hurricane Katrina have contributed to the maturation of the Department of Homeland Security, which is still a quite young department. We have learned, we have adjusted, and we have broadened partnerships across government, with the private sector and internationally. In some areas we have made tremendous strides, in others we have considerable distance to travel.

The most significant challenge we have is to continue the effort that was started with the creation of the new Department: merging 22 agencies with approximately 180,000 people and turning it into the most effective force to protect our country. This effort requires effective and efficient use of financial and human resources, enabling technology, strong processes and superb management. These are the challenges that are the focus of our efforts.
The major elements of our strategy are:

- Improving acquisition and procurement throughout the Department.
- Strengthening the requirements and investment review processes.
- Acquiring and maintaining human capital.
- Seeking efficiencies across the enterprise in operations and the use of resources.
- Making the key management systems, such as financial and information technology, world class.

Our approach has a common thread through all of these areas. That is to ensure that there is a comprehensive and integrated strategy with specific and measurable goals, and that these goals support the activities and priorities of the Department. On a practical level, we will ensure the success of this strategy by having a team with the right knowledge, skills and abilities to support these programs, the overall transformation and integration efforts. Our progress will be measured against metrics and milestones.

• How long do you think it will be before DHS can build and sustain the dynamic and effective integration that was envisioned for the Department?

Response: DHS was established to forge a new security capability built of some existing programs and some new ones, but all of them brought together into a dynamic new structure focused on meeting a new threat to our country. This was the largest government merger since the Defense Department was formed in 1947. While we are still working to organize ourselves in the most effective way, as evidenced by recent changes to FEMA and the Preparedness Directorate, we have largely settled on a firm construct that will provide the foundation for a well-functioning Department.

15. Four months ago, the President explained to the nation that immigration reform had to be comprehensive to be effective. He said "all elements of this problem must be addressed together, or none of them will be solved at all." Among the five essential elements he listed in his speech, he stated that undocumented immigrants who meet certain criteria must be eligible for citizenship. The criteria he listed would have conditioned eligibility for citizenship on people having had roots in their communities, paid penalties and their taxes, learned English, and held jobs. Those criteria for a path to citizenship were included in the bipartisan comprehensive immigration reform bill the Senate passed later that month.

• The Department of Homeland Security is responsible for providing immigration benefits, enforcing immigrations laws, and policing our borders. Do you agree with the President that our problems with respect to immigration enforcement and border security cannot be solved without also providing undocumented immigrants a path to earned citizenship? Please explain your answer.

Response: Effective enforcement of our immigration laws, and especially effective enforcement at the worksite, is closely connected with the creation of a program that will bring currently undocumented workers out of the shadows and under the rule of American law. This process must involve acknowledgement and atonement for those who have broken our immigration laws. No special path to citizenship should be created for individuals who broke our laws. Those individuals who meet a reasonable number of conditions and pay a penalty should be able to apply for citizenship, but approval would not be automatic, and they will have to wait in line behind those who played by the rules and followed the law.

• Recently the House and Senate leadership declared that comprehensive immigration reform legislation is dead, and that they intended to focus exclusively on border security and immigration enforcement. What is the Administration doing to try to overcome the opposition of House and Senate leadership to comprehensive immigration reform?

Response: The Administration is working with both Democrats and Republicans in Congress to find a practical answer to the important issue of immigration reform. I have had the chance to meet with many members of both the House and the Senate, and to hear their views on the main features of immigration reform. I look forward to working together with the Congressional leadership on sound and long overdue immigration reform legislation.

16. Improved border security is essential to repairing our broken immigration system, because any comprehensive reform must include more successful strategies for stopping illegal immigration. At the same time, credible evidence indicates that the greatest threat of terrorist infiltration into the U.S. is not from our Southwestern border. The 9/11 terrorists entered this country with visas awarded by US consulates and other terrorists have entered the U.S. through the Visa Waiver Program. We've spent billions of dollars on the US VISIT program, but that system is only as good as our terrorist watch lists, and it cannot stop terrorists traveling here under an assumed name unless we also know the alias or have their fingerprints. The Administration has not provided enough funding for our intelligence centers that process and

disseminate information about terrorist infiltration. Our first line of defense should be at our consulates, not our airports, but programs to improve training and screening at consulates have gone nowhere.

• What do you believe are our greatest vulnerabilities, with respect to the most likely routes for terrorist infiltration into the U.S.?

Response: Our enemies are resourceful. They are constantly probing our nation's defenses and looking for ways to exploit potential vulnerabilities. A multi-faceted, layered suite of security measures is needed to counter that threat. Verification of identity is paramount to securing our homeland. We must know who we are letting into our country. Document and identity fraud must be addressed aggressively. The Department recognizes that so long as the opportunity exists to mask one's identity, we cannot be safe. To this end, ICE, USCIS, US-VISIT, and the Department are working to mitigate vulnerabilities. Through technology and enhanced inspection tools.

Another vulnerability is the financing of terrorism. Those who fund the groups that commit acts of terrorism are no better than the terrorists themselves, and they must continue to receive focused attention. The Department has partnered with our counterparts at the Department of the Treasury and others to identify means that might be exploited by those seeking to bring harm to our homeland.

The presence of organized crime likewise remains a vulnerability. These criminal rings are driven by greed, and the potential for terrorists to exploit such organizations to facilitate their fanatical agendas cannot be ignored. We must continue to dedicate manpower to the eradication of these highly sophisticated criminal organizations.

• What has DHS done to develop a comprehensive strategy for detecting and preventing terrorist infiltration through all avenues, not just across the Mexican border? What have you done to implement that strategy?

Response: DHS has a comprehensive and layered approach to ensuring protection of our borders. The Secure Border Initiative, coupled with the efforts of other DHS entities, ensures that the best possible steps are being taken to both detect and prevent terrorist infiltration.

The challenge for national security in an age of terrorism is to prevent the people who may pose unacceptable risks from entering or remaining in the United States undetected. Presently, DHS captures biometric information on entry through the United States Visitor and Immigrant Status Indicator Technology (US-VISIT) Program. US-VISIT verifies the biometrics of travelers with visas, who are fingerprinted abroad by the Department of State as part of the biovisa program. The use of biometric identifiers – specifically digital fingerprints and photographs – has made travel safer and more secure by allowing DHS and DOS to identify persons attempting to enter the United States using fraudulent identities and screen individuals to determine whether they constitute a risk to national security. These biometrics are used to fix the identity of an

individual during his or her first encounter with the U.S. Government, to verify the identity of the individual upon subsequent encounters, and to run appropriate watch list checks on the individual if he or she is seeking immigration benefits or admission to the United States.

The Department's border-security efforts extend far beyond US-VISIT. The Secure Border Initiative (SBI) is a comprehensive multi-year plan to secure America's borders and reduce illegal immigration. Through SBI and other efforts, DHS is strengthening security along our northern and southern borders through the integrated use of increased manpower and infrastructure, cutting-edge technology, enhanced immigration enforcement, and cooperation with our state and local partners. Specifically, SBI includes:

- More agents to patrol our borders, secure our ports of entry and enforce immigration laws;
- Expanded detention and removal capabilities to eliminate "catch and release" once and for all;
- A comprehensive and systemic upgrading of the technology used in controlling the border, including increased manned aerial assets, expanded use of UAVs, and next-generation detection technology;
- Increased investment in infrastructure improvements at the border – providing additional physical security to sharply reduce illegal border crossings; and
- Greatly increased interior enforcement of our immigration laws – including more robust worksite enforcement.

The Administration is looking at technological and infrastructure enhancements that will help to both detect and prevent infiltration. Through the SBInet DHS will use technology to secure our borders. The use of radiation detectors, sensors, cameras, and biometric information dramatically increase the likelihood of apprehending criminal or terrorist elements attempting to enter the U.S. through both our southern and northern borders.

While welcoming all legitimate travelers and trade, CBP officers and agents enforce all applicable U.S. laws. All legal visitors and returning Americans, as well as sanctioned cargo, enter the U.S. through one of 314 land, air or seaports. CBP's immigration inspections are important to enforcing U.S. immigration laws and assuring border security. In addition to a number of operations on the Southern border, such as Operation Jumpstart and Streamline, CBP has increased its manpower on the Northern border. This increase in manpower improves CBP's ability to detect, apprehend, and deter illegal aliens, criminal elements, and terrorist threats along the border with Canada.

U.S. Immigration and Customs Enforcement works closely with the Joint Terrorism Task Forces (JTTFs). ICE is the second-largest federal contributor to the nation's JTTFs with more than 300 ICE agents assigned to task forces nationwide. ICE also conducts investigations involving the illegal export of U.S. arms and strategic technology, including Weapons of Mass Destruction. ICE also is working collaboratively with U.S. Citizenship and Immigration Services to fight identity fraud.

• In the overwhelming majority of countries and consulates, there are no DHS officers deployed. As long as that situation continues, shouldn't DHS be doing more to help train State Department consular officers in the various methods used to investigate and screen visa applicants for possible terrorist ties? What programs does DHS currently have in place in this area, and what funds has DHS committed to the programs?

Response: In accordance with Section 428 of the Homeland Security Act, which authorizes DHS to provide advice and training to Department of State (DOS) Consular Officers at post, the ICE Office of International Affairs, Visa Security Unit (VSU) deploys Visa Security Officers (VSOs) at visa-issuing posts. These VSOs provide day-to-day, case-specific advice and formal training as needed to DOS Consular Officers. They also share their expertise in immigration law, counterterrorism, document review, fraud detection, interview techniques, and other skills relevant to the successful adjudication of visa applications.

VSOs provide effective consular advice and training through their day-to-day interaction with Consular Officers during the course of their adjudicative work. At the posts where they are deployed, the VSOs have developed strong working relationships with the Consular Officers, who routinely consult with them during their adjudication activities. As the VSU expands, it will provide training at each new post where it is deployed.

The VSU provides briefings regularly at the Foreign Service Institute (FSI), the VSOs conducting these briefings are law enforcement officers who bring extensive subject matter expertise to the visa issuance process. VSOs interpret, evaluate, and effectively apply the full range of information available from law enforcement and other systems. The VSU provides training to overseas ICE personnel in VSU techniques and activities and has trained ICE overseas personnel in its Europe, Middle East, Africa, and Asia. Funds for formal and informal training are included in the overall VSU budget and funding for FY 2007 is $15 million.

• Why did the Administration propose to cut the budget for FY07 for the ICE Office of Intelligence, which contains the Anti-Terrorism Unit and the Human Smuggling and Alien Intelligence Unit? Will you urge the President to restore funding for this office?

Response: The FY 2006 budget for ICE Intelligence was $52,256,000. This included $50,460,000 from initial appropriations plus $1,796,000 from the Hurricane Katrina Supplemental. The Hurricane Katrina Supplemental was one-time funding. When taking this one-time funding into account, the $51,379,000 budget for Intelligence in FY 2007 is an increase of $919,000 over FY 2006.

17. A major study by the National Academy of Sciences in 2002 warned that to harden our defenses quickly: "It is important…that the federal government define a coherent overall strategy for protecting the nation, harness the strengths of the U.S. science and engineering communities, and direct them most appropriately toward critical goals, both short-term and long." In creating the DHS Directorate of Science and Technology (S&T), Congress wanted DHS to take the lead in coordinating federal R&D against the WMD attacks. The Strategic Plan was supposed to be

the lynchpin of this work, a roadmap for our National Laboratories, research universities and the private sector.

• Did DHS develop this Strategic Plan and use it in 2005 to guide federal R&D against chemical, biological and nuclear terrorist threats and is it being used today?

Response: In addition to developing a government-wide strategic plan for homeland security science and technology, the Science and Technology (S&T) Directorate participates in several interagency working groups to identify gaps and avoid duplicate efforts in Federal research and development (R&D). These interagency working groups provide input on policy and research issues to help assure that funding is requested in the appropriate areas of R&D throughout the Federal government.

The S&T Directorate has been working through the interagency process to develop the government-wide *National Plan for Homeland Security Science and Technology,* which articulates the Nation's strategic vision for science and technology in support of homeland security, as well as identifying key near-, mid-, and long-term priorities that will help make this vision a reality. The *National Plan for Homeland Security Science and Technology* serves as a foundation for the development of comprehensive, research-based definable goals for such efforts and development of annual measurable objectives and specific targets to accomplish and evaluate the goals for such efforts. The plan was placed in the final informal interagency review in the fall of 2005 and the comments and changes are currently being incorporated. The Plan will be submitted for Departmental clearance and then interagency clearance led by OMB in the coming months.

• Does it include measurable research targets and have our R&D investments been meeting those goals?

Response: The *National Plan for Homeland Security Science and Technology* serves as a foundation for the development of comprehensive, research-based definable goals and development of annual measurable objectives and specific targets to accomplish and evaluate the goals for such efforts. In addition, the Department's Strategic Plan sets Departmental goals and objectives that guide the S&T Directorate's R&D investments.

• Both GAO and Committee staff have asked the S&T Directorate for a copy of the Strategic Plan – so far to no avail. Will you provide this Committee with a copy of the plan?

Response: The *National Plan for Homeland Security Science and Technology* will be a publicly available document after it has completed Departmental and inter-agency review.

18. The requirement that DHS develop a Strategic Plan for R&D reflected a major post-9/11 reform, but it was also supposed to drive the work of your S&T Directorate. I am concerned that warning signs of trouble in the S&T reflect a failure at DHS to take this work seriously. The Homeland Security Science and Technology Advisory said in its Annual Report that the S&T

Directorate's "Strategic Planning process is underway," but needed more staff, better metrics and methodology and clearer guidance on research priorities. This past June, the Senate appropriators called the S&T Directorate "a rudderless ship without a clear way to get back on course" and directed DHS "to immediately develop a 5-year research plan," reflecting DHS' research and funding priorities, because "developing and implementing this 5-year plan is the only way S&T will be successful." Why is this Directorate's performance less than Congress intended and what steps will you take to improve it?

Response: The Science and Technology (S&T) Directorate is improving its business approach by streamlining processes, improving accountability and empowering people. The S&T Directorate is implementing this improved business approach through its Planning, Programming, Budgeting, and Execution (PPBE) process, which encompasses the development of strategy, priorities, program plans, resource requirements, and associated performance metrics. The PPBE process is a continual cycle that drives the organization to evaluate strategies, refine its resource allocations, and ensure that it remains accountable. Outcomes of this process will be reflected in a 5-year research and development plan that will outline our strategic direction, detail all of our R&D programs, and set out a performance measurement approach to ensure accountability.

In addition, to improving its business approach, the S&T Directorate is implementing many changes that will enable it to be a more responsive, agile, customer-focused organization -- one that better enables our Nation to prevent, protect, respond, and recover from acts of terrorism, natural disasters or other emergencies. These changes include new leadership, an aligned organizational structure and further focusing the work of the S&T Directorate.

In August, the Senate confirmed Jay M. Cohen as the new Under Secretary for Science and Technology. Under Secretary Cohen brings vast scientific expertise and critical leadership to the Department having recently served as Chief of Naval Research, commanding the Office of Naval Research and managing science and technology programs for the Navy and Marine Corps.

Under Secretary Cohen has already aligned the S&T Directorate and supports a clearly defined mission for the S&T Directorate: to protect the homeland by providing Federal, state, local, and tribal officials with state-of-the-art technology and resources. The S&T Directorate will accomplish this by:

- Developing and deploying state-of-the-art, high performance, affordable systems to prevent, detect and mitigate the consequences of chemical, biological, and explosive attacks;
- Developing equipment, protocols, and training procedures for response to and recovery from chemical, biological, and explosive attacks;
- Enhancing the technical capabilities of the Department's operational elements and other Federal, State, local and tribal agencies to fulfill their homeland security related missions;
- Developing methods and capabilities to test and assess threats and vulnerabilities, and prevent technology surprise and anticipate emerging threats;

- Developing technical standards and establish certified laboratories to evaluate homeland security and emergency responder technologies, and evaluate technologies for SAFETY Act protections; and
- Supporting U.S. leadership in science and technology.

The S&T Directorate has a significant role in bringing to bear solutions to the Department's homeland security challenges. These and other changes will provide the Department with an S&T Directorate that is easier to access, so that homeland security personnel can utilize technologies and solutions that will make their jobs better, more efficient, more cost effective, and safer.

19. The Department's prolonged failure to nominate an Assistant Secretary for Cyber Security and Telecommunications appears to be symptomatic of a larger hiring and retention problem at the Department that spans all levels of executive and mid-level management. Recent comments by Assistant Secretary for Intelligence and Analysis Charles Allen – specifically, that DHS is suffering from a lack of all source intelligence analysts at the GS 12-14 level – and from FEMA Director David Paulison – that efforts to staff FEMA at 90 percent before the June 1 start of the 2006 hurricane season were not met due to cumbersome hiring practices – are other examples. If the Department is unable to hire or retain mid-level managers, its ability to build a solid, lasting foundation for carrying out the Department's vital homeland security mission will be compromised.

• Please provide FTE vacancy reports for the Department, broken down by office within each Directorate or Component, and further broken down by GS grade.

Response: The following table provides information on FTE, within the Department of Homeland Security, as of the end of 3rd Quarter FY 2006. For most of these vacancies GS levels are yet to be determined and are routinely determined by classification experts immediately preceding the vacancy being announced.

Questions for the Record
Senate Homeland Security & Governmental Affairs Committee
"Homeland Security: The Next Five Years"
All responses are current as of the date of the hearing: September 12, 2006
Secretary Michael Chertoff

DHS Department-wide Employment Report

Rev. as of 8.29.06

	POSITIONS (CIVILIAN)			VACANCIES					POSITIONS (MILITARY-Active Duty)			DETAILEES ON BOARD**		
ORGANIZATION/ COMPONENT	FY06 Total	On Board	Vacant	Recruiting In process	Selections Made/Tentative Offer Made	Pending Security	Pending EOD	Other*	Total	On Board	Vacant	Civilian	Military	COMMENTS
FEMA	2,215	1,808	407	311	16	54	22	26	0	0	0	5	2	
FLETC	1,255 [1]	1,160 [1]	95 [1]	68	12	3	12	0	0	0	0	140	6	
HQ*	2,441	1,873	574	197	22	114	49	28 [2]	0	0	0	0	0	[3]
OIG	542	495	47	29	6	3	8	1	0	0	0	0	0	[4,5]
TSA	54,309	51,794	2,515	403	267	115	220	0	0	0	0	0	0	
USCBP	34,469	42,622	[7]	3,386	1,076	1,076	500	0	0	0	0	26	6	[6,7]
USCG	7,750	7,298	452	329	46	9	68	0	40,771	40,830	0	0 [8]	0 [8]	
USCIS	8,690	8,713	[9]	58	34	163	35	0	0	0	0	1	0	[9]
USICE	16,568	14,928	1,640	1,313 [10]	836 [11]	1,104	360	174 [12]	0	0	0	4	0	[13]
USSS	6,564	6,496	68	83	90	191	77	4 [14]	0	0	0	2	0	[15]
Totals:	134,803	137,187	5,798	6,177	2,405	2,832	1,351	233	40,771	40,830	0	178	14	

* *HQ Statistics include: CIS-OMB, CRCL, Exec Sec, OGC, OLA, OPA, OPS, OS, Policy, Privacy, US-VISIT, DNDO, S&T, Preparedness & USM (see attached drill down for details within HQs)*

** *Detailees to DHS from other agencies; do not report detailees between DHS components/HQ organizations.*

[1] Includes reimbursable positions
[2] 25 declined; 3 cancelled
[3] Does not include I&A
[4] Data does not include Katrina FET's (FET's - 97; Filled - 36; Recruiting in Process - 54; Selected Pending Security - 7)
[5] Some audit vacant positions are on-hold until 7/26/06.
[6] A/O 1st Q. FY06
[7] CBP manages to budget and does not maintain data on vacancies. Numbers reflect recruitment actions pending in the Personnel Actions database (PARTS) and not all vacancies in CBP.
[8] Detailee #'s will be submitted on 6/30
[9] CIS manages to budget. The 8,690 reflect the budgeted positions for FY-07. FY-06 is an anomaly because of the end of the backlog elimination project. As a result, no FY-06 levels were authorized, but rather, in January 2006, CIS issued FY-07 budget lev

[10] Some of these numbers appear to be inconsistent as ICE makes a greater number of tentative selections than the total number of recruit actions authorized. This is because for every 4 candidates provided with a tentative offer, on an average, only one will

[11] 1200 additional offers being made by the Minneapolis Hiring Center by June 30, 2006
[12] Pending Waivers/PCS.
[13] ICE's vacancies reflect supplemental and enhancement positions (FY 05 and 06) that are still being filled. In addition this number is the result of significant time delays in getting staff in place based upon prior hiring restrictions and security proces

[14] Hold pending updated information
[15] Due to anticipated attrition and failure rate in the background process, USSS over-recruits for positions

• What strategies is the Department pursuing to ensure that it hires and retains a well-qualified mid-level management and analysis workforce?

Response: As part of its overall workforce planning strategies, the Department has developed a multi-tiered leadership curriculum to ensure that individuals in Supervisory and Managerial positions receive the appropriate training at all levels to manage programs, analyze continuing requirements, and carry out the mission. In addition, competencies are being identified for positions within the Department as part of the effort to establish a competency-based qualifications system. Once implemented, DHS will be the only Department in the Federal government to qualify all applicants for positions based on validated competencies.

• What steps are the Department taking to reduce staffing delays caused by the lengthy hiring cycle?

Response: The Office of the Chief Human Capital Officer is working closely with the components to develop a comprehensive approach to improving the hiring process Department-wide. This multi-layered effort will include; ensuring that vacancy announcements are professional, clear, and compelling, use of assessment instruments that have a greater ability to predict future performance and make finer distinctions among candidates, implementation of an enterprise E-Recruitment system to better manage the process, evaluate hiring processes, procedures, and policies to identify barriers by utilizing the Hiring Toolkit recently developed by OPM, and make better use of existing hiring flexibilities such as Category Rating, the Federal Career Intern Program and Veterans' hiring authorities. This effort will take place throughout FY07.

• What steps are the Department taking to recruit for hard-to-fill CxO (Chief Financial Office, Chief Information Office, and Chief Procurement Office), intelligence analyst, and FEMA positions?

Response: All of the Line of Business Chiefs have embarked on Workforce Planning and Recruitment efforts to close their hiring gaps. In addition, the Chief Procurement Officer has hired a Director of the Acquisition Workforce, to oversee workforce planning and recruitment efforts Department-wide. Using the Federal Career Intern Program the CPO has developed the DHS Acquisition Fellows Program in order to hire individuals at the entry-level and train and develop these individuals to become Contract Specialists. The Office of the Chief Human Capital Officer has prepared a comprehensive Human Resources Improvement Plan that addresses those competency gaps identified through the recent Human Resources Competency Assessment. The plan also establishes a curriculum for training HR Specialists at all levels and; will utilize the Federal Career Intern Program to fill vacant positions in the HR arena. The Intelligence and Analysis Directorate has embarked on a comprehensive recruitment campaign to fill its hard-to-fill positions to include attending targeted recruitment events for individuals with security clearances; participating in diversity recruitment events and activities to recruit individuals with disabilities, minorities, and veterans for vacant positions; participating in on-campus career fairs at colleges and universities to recruit individuals with diverse skills and education and; participating in the Presidential Management Fellows Program to develop individuals for future leadership positions. An effort is also underway within FEMA to utilize the U.S. Office of Personnel Management's USA Staffing system to assist FEMA in filling its vacant positions in a more efficient and effective manner.

20. To create a true homeland security culture, DHS must avoid an over-reliance on using contractors in lieu of a stable, permanent workforce. The initial creation of such a large Department clearly required that contract support be used as an emergency fix to ensure the Department functioned effectively. However, such support must be used as a temporary stop-gap measure rather than as a permanent solution to staffing shortfalls.

• Please provide a report detailing the number of private-sector contract employees at the Department, broken down by office within each Directorate or Component.

Response: DHS does not track contractor FTE because we often acquire support on a fixed price basis or based on performance objectives. The number of personnel the contractor employs is not transparent or relevant since we are paying for a deliverable or outcome rather than man-hours. In those instances where DHS is acquiring a specific "level of effort" or man-hours, contractors may use several employees to accomplish tasks that total the number of man-hours in one FTE. Thus, it is not possible to track or provide this information.

• What, if any, steps is the Department taking to phase out any contract support positions or convert those positions into more cost-effective FTEs?

Response: As part of the Department's Workforce Planning efforts, each Office and Component is responsible for determining the best manner in which to close competency gaps in their mission critical positions. Closing competency gaps can occur through training and development initiatives; recruiting and hiring efforts; or the contracting of certain functions to private sector organizations. As determinations are made that Full-Time Equivalent civil service positions are more efficient and effective in meeting mission requirements, positions are requested through the annual budget process.

21. Based on revisions to the National Response Plan, the new National Operations Center (NOC) framework includes an Incident Advisory Council (IAC) to replace the Interagency Incident Management Group. The IAC is charged with adjudicating unresolved resource issues and providing strategic advice during an actual or potential Federal disaster response. Unfortunately IAC membership has not yet been established, nor has the Council been integrated into the overarching Federal response structure.

• When will the IAC's final composition be determined?

Response: The proposed Incident Advisory Council (IAC) was never established due to concerns about the potential for redundancy and duplication of effort with an existing body, the Domestic Readiness Group (DRG). The Assistant Secretary-level DRG, which meets weekly, will also be stood up as needed in response to major incidents.

• What steps will be taken to integrate the IAC into the NOC framework? Is there a timeline for final integration into the NOC framework?

Response: Please see above response. In addition, when the Assistant Secretary-level DRG is activated, the NOC will provide administrative, logistical and operational support to this body.

22. On September 21, 2006 the SBInet contract was awarded to Boeing Co. one of the five prime contractors competing for the project, which is expected to cost billions of dollars to implement. Under the Secure Border Initiative, DHS had earlier announced that it would be hiring a contractor to come up with an integrated solution "which addresses all aspects of border security." DHS offered contractors no opinion as to how this goal should be accomplished. At a conference in January 2006, Deputy Secretary Michael Jackson told industry leaders, "I want to make sure you have it clearly, that we're asking you to come back and tell us how to do our business." Why is DHS delegating to a contractor such broad responsibility for formulating a comprehensive border security strategy? Why don't you believe these decisions are best left to DHS officials?

Response: The government is not delegating comprehensive border security responsibilities to a contractor, nor is this what Deputy Secretary Jackson intended with his remarks. SBI*net* is an important element in the Department's Secure Border Initiative. The Department asked industry to propose solutions that would aid in securing the borders by detecting, identifying, and classifying incursions, and apprehending individuals committing cross-border crimes. The optimal solution is one that will utilize a mix of personnel, technology, and tactical infrastructure to control 6,000 miles of border. The overall requirements and strategies for securing our borders are firmly the domain of the government.

23. According to recent stories in the Washington Post (dated September 18 and September 20), the five prime contractors bidding for the SBInet project offered radically different border security strategies. According to the Post story (which quoted executives of the bidding corporations), Northrop Grumman Corp. proposed to rely heavily on unmanned aerial aircraft. Ericsson Inc. would have emphasized the use by Border Patrol officers of wireless devices capable of receiving live video. Lockheed Martin Corp. would have placed a bigger emphasis on blimps. Raytheon Co. proposed equipping Border Patrol vehicles with real-time access to sensor activity and video feeds. The eventual winner, Boeing Co., proposed a series of towers lining the borders. The award for the SBInet was made after competitive bidding. But the advantage of competitive bidding is that it allows the government to determine that it is getting the best value for whatever goods and services it procures. In this case, the five prime contractors were offering completely different products and services, and the contracting officers were presumably comparing "apples and oranges." How can DHS know, now and in the future, that the winning contractor charges a fair price for the border strategy solution it implements?

Response: It is not accurate to say that the SBI*net* bidders offered completely different services. While not the same, they were, in fact, comparable in overall ability and effort. Comparisons were based on an evaluation of each proposed solution's likely effectiveness in deterring, classifying and apprehending illegal border entries. The evaluation was based on eight factors that were, in turn, based on the performance measures quality assurance plan. This quality assurance plan requires the contractors to identify and quantify measures and metrics for achieving overall program objectives. Those measures and metrics, based on technical solutions, enabled the government to individually assess the effectiveness of each offeror's solution. In addition, each offeror proposed initial tasks that would demonstrate the feasibility of the overall

solution to the goals and metrics that task would achieve. Finally, we considered each offeror's cost and price proposal for reasonableness, realism, and price risk. The final selection was based on a best value approach for the government.

24. We recently observed the solemn one year anniversary of the landfall of Hurricane Katrina. Shortly after the storm hit, President Bush made a commitment to help the people of the Gulf Coast rebuild their communities. But one year after the storm, thousands of evacuees are not receiving the help they need, housing remains in short supply which frustrates the ability of residents and businesses to find employees, and many neighborhoods still look like the storm hit just a few weeks ago, rather than a year ago. Almost everyone is frustrated and the mental strain is overwhelming for many, many people who still face uncertain futures. In short, victims of the storms are suffering because of the many problems with the recovery. These issues pose a significant series of critical challenges that must be resolved, or at least contained, before the wind blows new perils. While no one should expect that any region can recover from such a huge, devastating storm overnight, the American people have a right to expect a far more vigorous response from FEMA and much more leadership from the federal government. Are you satisfied with DHS' efforts on assisting with the recovery? What is your plan to help turn around the recovery?

Response: FEMA and DHS continue to provide leadership for the recovery of the Gulf Coast Region. FEMA appointed Gil Jamieson as Deputy Director for Gulf Coast Recovery to establish Transitional Recovery Offices in each of the impacted states. Transitional Recovery Offices (TROs) administer FEMA's recovery and mitigation programs in the field. FEMA's Gulf Coast Recovery Office is the primary interface between FEMA and the President's Coordinator for Gulf Coast Rebuilding, Donald Powell.

FEMA coordinates the involvement of federal agencies in the recovery through mission assignments and inter-agency agreements. While hundreds of mission assignments for response and early recovery operations have closed out, FEMA continues to have 16 operationally active mission assignments, and 27 active inter-agency agreements (as of 9/30). These agreements include activities with: US Army Corp of Engineers, US Coast Guard, US Department of Transportation, Federal Protective Service, Tennessee Valley Authority, General Services Administration, Department of Defense, Environmental Protection Agency, Department of the Interior, NASA, and Health and Human Services.

The Gulf Coast Recovery Office (GCRO) works closely with the Office of the Federal Coordinator on numerous issues, including resettlement of displaced residents, effective program delivery, and ensuring state and local governments maximize federal programs and services.

In terms of support for long-term community recovery, GCRO has staff working on the ground to help local communities implement the recovery plans developed by Emergency Support Function 14 (long-term community recovery). GCRO has also provided technical support to recovery expos and resource fairs in Mississippi and Louisiana.

The Gulf Coast Recovery Office, which manages the four Transitional Recovery Offices (AL, LA, MA, TX) has authorization for 2593 CORE employee positions. Unlike response phase positions, in which there is frequent rotation of staff, CORE appointments are tailored to the recovery phase of gulf coast operations, lasting up to two years. As of September 13, 2006, GCRO had reached 67% of its target staffing level. Through its hiring of CORE employees, FEMA stimulates local economic recovery as many of the CORE staff are from areas impacted by the hurricane.

FEMA is committed to helping communities build back stronger and more sustainable communities. Through the TROs, FEMA will continue to support the Gulf Coast states and local communities in their recovery efforts.

25. Almost exactly one year ago President Bush's stood in Jackson Square, New Orleans and pledged to put the full might of the federal government behind the citizens of the Gulf Coast to help them recover from the devastation of Hurricane Katrina. Some of the President's exact words were "We will do what it takes. We will stay as long as it takes." He also said, "American wants the Gulf Coast not just to survive, but to thrive, not just to cope, but to overcome." Despite these comments, most of the assessments of the recovery effort indicate that the President's promises are not being fulfilled. Do you need additional authorities to fulfill President Bush's promises?

Response: The scope and magnitude of the Katrina and Rita hurricanes presented the Agency with many unique challenges. FEMA will continue to work with The Department to review Stafford Act Authorities, and, if necessary, propose changes to strengthen FEMA's disaster relief program.

26. One of the key components of the coordination described in the National Infrastructure Protection Plan (NIPP) is the effective sharing of information between all levels of government, including international governments, and between the public and private sectors. In particular, the NIPP stipulates that as partners in the Sector-Specific Councils, the private sector must pass information to the government in return for threat and security information. The Government Accountability Office reported in April 2006 ("Information Sharing: DHS Should Take Steps to Encourage More Widespread Use of Its Program to protect and Share Critical Infrastructure Information", GAO-06-383) that significant impediments to the private sector's willingness to share information with the government remain. DHS concurred with GAO's report of these private sector concerns.

• In light of these concerns, and DHS's concurrence, what measures has the Department taken, or intends to take, in order to address the impediments? Has DHS has acted on GAO's "Recommendations for Executive Action" as detailed in the report, and if not, why not? What other actions has DHS taken?

Response: In April 2006, after a review of the implementation of the Critical Infrastructure Information Act of 2002 (CII Act), the Government Accountability Office (GAO) released a

report entitled *Information Sharing: DHS Should Take Steps to Encourage More Widespread Use of Its Program to Protect and Share Critical Infrastructure Information* (GAO-06-383). In the report, GAO assessed the efforts of DHS to implement the CII Act and the challenges DHS continues to face in doing so.

The GAO report recommends several changes that DHS or the Protected Critical Infrastructure Information (PCII) Program Office could make that might increase submissions of critical infrastructure information (CII) and provide incentives for more widespread use of PCII. This response details the PCII Program Office's efforts in those areas. The recommendations made by GAO fall into five broad categories:

- Issuing the Final Rule
- Providing clarity regarding how submitted CII will be protected
- Establishing some level of originator control
- Allowing indirect submissions
- Providing a mechanism for state-to-state sharing

In addition, the GAO report recommended other executive actions that are beyond the purview of the PCII Program Office and fall within other DHS components, notably defining and communicating to the private sector what CII DHS and Federal entities need and how they anticipate using such CII. The PCII Program is an information sharing tool that works in conjunction with other information sharing programs such as the NIPP to increase information sharing between the private sector and government. As such, the PCII program's mandate does not consist of defining DHS' CII requirements.

Issuing the Final Rule
The Final Rule (6 CFR Part 29, *Procedures for Handling Critical Infrastructure Information; Final Rule*), under which the PCII Program is currently operating was published and became effective on September 1, 2006.

Providing clarity regarding how submitted CII will be protected
According to the GAO report, "potential submitters often continue to be reluctant to provide their sensitive information because they are not certain that their information will be fully protected[1]." The PCII Program Office employs a variety of methods to communicate its policies. In order to improve the communication of the program's information safeguarding procedures, the PCII Program Office has established a Policy Working Group to distill the protections afforded PCII by the CII Act of 2002 into succinct policies. Once the Policy Working Group has elucidated these policies, the PCII Program Office is better able to clearly communicate them. All briefings by program officials to private industry groups feature a thorough overview of PCII safeguarding procedures. In addition, the PCII Program has a Web page that is currently being updated to reflect changes made to the program by the Final Rule. All visitors to the PCII Web

[1] *Information Sharing: DHS Should Take Steps to Encourage More Widespread Use of Its Program to Protect and Share Critical Infrastructure Information* (GAO-06-383), p. 19.

page will have the opportunity to get additional information about the program's safeguarding objectives and procedures. Furthermore, anyone needing additional information about the program can contact the PCII Program Office with questions either via phone or through a dedicated e-mail address pcii-info@dhs.gov.

The PCII Program Office has placed articles in many publications detailing the program's utility to potential submitters, as well as information about the policies and procedures in place to safeguard PCII. These articles have been widely circulated in trade publications and journals. The GAO report mentions the PCII Program Office's success in promoting the program, specifically noting the more than 30 articles that have appeared in trade publications discussing the program. Since the end of the GAO's review, an additional nine articles were published in trade publications and has had several more distributed on portals and listservs.

Establishing some level of originator control
In response to feedback from private sector groups, the PCII Program Office allows submitters to limit the parties that will have access to their submitted information. Even under the limited dissemination arrangement, however, the wishes of the submitter will be carried out only to the extent possible and may be overridden by the PCII Program Manager under specified conditions (i.e., when the information is needed in exigent circumstances or by operational necessity). Ultimately, the PCII Program Manager will decide whether or not circumstances dictate that PCII should be shared.

Allowing indirect submissions (submissions made directly to agencies other than DHS)
The Final Rule allows for Federal agencies other than DHS to receive CII on behalf of DHS, provided that such CII is then passed to the PCII Program Office for validation. These types of submissions are knows as "indirect submissions". In addition, the Final Rule gives the PCII Program Manager the discretion to declare certain subject matter or types of information categorically protected. Such information will be considered validated as PCII upon receipt by either the PCII Program Office or a designee of the PCII Program Manager. The Final Rule defines a "designee" as a Federal employee whether employed by DHS or another Federal agency, to whom certain functions of the PCII Program Office are delegated by the PCII Program Manager. These mechanisms allow for more expansive and flexible CII collection, while preserving the PCII validation role for the PCII Program Manager. The PCII Program Manager will normally only allow indirect submissions when the particular governmental entity has: (1) appointed a PCII Officer; (2) the necessary staff, who are trained in PCII procedures; (3) implemented measures to comply with the Final Rule; and (4) agreed that the PCII Program Office may at any time verify that agency's compliance with the Final Rule and other program requirements.

Providing a mechanism for state-to-state sharing
Under the Interim Rule, State and local government officials were prohibited from sharing PCII with other authorized users, including their contractors, unless permission to do so was obtained from the submitter. The Final Rule addresses this barrier to information sharing by allowing State and local government officials to share PCII with other parties already authorized to

receive such information by the PCII Program Manager. The PCII Program Office has developed an accreditation program as a means to share PCII with eligible government entities effectively and consistently. The accreditation program has been designed to ensure the proper handling, use, dissemination, and safeguarding of PCII by government users. A State or local entity can become authorized to receive PCII once its accreditation process has been initiated. In addition, State or local entities may share PCII with users who are not authorized to access PCII, but only after obtaining authorization to do so from the PCII Program Manager or Designee, who are responsible for requesting written consent from the submitter.

The PCII Program Office has already accredited the States of Arizona, California, Massachusetts and Maryland to receive PCII and is currently working with 21 other State and local entities to get them accredited including, New York State, New Jersey, Virginia, the District of Columbia, and the cities of Indianapolis, Las Vegas and Seattle. Once they are fully accredited, the changes made in the Final Rule will facilitate information sharing amongst these entities, should they want to share PCII.

27. The administration has not yet submitted a plan for the Information Sharing Environment (ISE), as required by the Intelligence Reform and Terrorism Prevention Act of 2004. Because the sharing of information is critical to the success of the NIPP, absence of such a plan would be expected to have a deleterious effect on the effective implementation of the NIPP.

• Please explain the measures that DHS has taken, in the absence of a clear and precise national strategy for the sharing of information between the many agencies, levels of government, and sectors involved.

Response: Within the context of the NIPP, information sharing is an enabler to accomplish its stated overarching national goal. The NIPP describes an information sharing framework which consists of the following elements: outcomes/results that need to be enabled, content creation structures and processes tailored for critical infrastructures and key resources (CI/KR) protection and risk management, information delivery and coordination mechanisms, and governance and coordination structures and processes that build "trust", a foundation for effective information sharing. The principles of the ISE are integrated into this framework.

Defining outcomes/results in the NIPP, by mitigating national risk to the CI/KR, drives what information needs to be shared and in what form to make it useful and actionable. It also determines who needs that information in order to take appropriate action. The Homeland Information Threat and Risk Assessment Center (HITRAC) provides for the fusion of threat, vulnerability and consequence information. The National Infrastructure Coordinating Center (NICC) and the Homeland Security Information Network for Critical Sectors (HSIN-CS) provide the coordinating and technological mechanisms for delivery of information, as well as mechanisms through which information from CI/KR owners and operators can be reported. To facilitate the latter, the final rule to implement the Protected Critical Infrastructure Information Act was issued in September. The essential element for free and timely flow of information is trust building. This trust is dependent on a true public-private partnership structure and

processes. The NIPP describes the Sector Partnership Model which is inclusive of all levels of government with a role in CI/KR and the owners and operators of the CI/KR. That structure was formally recognized in March 2006 through the establishment of the Critical Infrastructure Partnership Council (CIPAC). Members of this partnership, in both government and the CI/KR sectors utilize or coordinate with the elements of the CI/KR information sharing framework. All of its elements have moved into production and operation. As the ISE plan is issued, the structures and processes for this CI/KR information sharing framework will adapt to its requirements.

• Please explain, in specific terms, how the lack of a plan for ISE has affected the current implementation of the NIPP, and how completion of the ISE plan can be expected to aid implementation.

Response: The NIPP was issued in June, 2006. All elements of the required CI/KR information sharing framework, as described in the previous response and as described in the NIPP have been implemented. These elements are basic foundations for an effective information sharing environment. The issuance of the ISE plan will strengthen these structure and process elements by providing consistency through standardization of and clarity on flow and management of sensitive information from both government and the CI/KR owners and operators. It can enhance capability to fuse more information than currently available to provide a more accurate picture of risk for the CI/KR sectors. By facilitating more efficient sharing of information within the federal government and with other levels of government with which the CI/KR owners and operators must interact to take action to mitigate risk, it provides for better communication and coordination of investments to prepare for and respond to events.

RESPONSE TO:
Post-Hearing Questions for the Record
Submitted to the Honorable Leroy D. Baca
From Senator Susan M. Collins

"Homeland Security: The Next Five Years"
September 12, 2006

1. ***You have described in detail policies and procedures that have worked well in Los Angeles. It goes without saying that there a number of characteristics of both cities that are unique or at least limited to similar, major metropolitan areas.***

   Of the observations and suggestions that you have made in your testimony today, what lessons have you learned that you believe can be applied to law enforcement departments in other metropolitan areas and even smaller communities across the Nation?

   The most profound lesson to be learned from the Southern California experience is that no single department, agency, or discipline can manage all the issues necessary to ensure a secure homeland. It is only through the building of relationships within public safety organizations, private sector supporters and non-governmental organizations that we can achieve a measure of security.

   The Los Angeles Joint Regional Intelligence Center (JRIC) is an example of one structure that seeks to incorporate these disparate resources into the intelligence process. Comprised of members from law enforcement, fire service, public health and the Department of Homeland Security, the JRIC seeks to extend its reach into the private sector and the community at large. Programs such as Infraguard and the Private Sector Terrorism Response Group (PSTRG) have made great inroads into energizing the private sector to become additional eyes and ears for indicators of terrorist activity. Similarly, the Muslim American Homeland Security Congress is an effort to reach out to the community for their support in fighting extremism in our society. All of these initiatives are available for replication across the country as they can be scaled for the size of the operation and/or the population served.

   The main points to be considered are the necessity for federal, state and local law, fire and health agencies to work together, the need to involve the private sector, and the requisite outreach to local communities. Input from these three critical components is essential to making a difference in the safety of any jurisdiction.

2. ***You have talked about the great progress your respective entities have made in the area of homeland security. There are still, of course, a number of areas where cities could be targeted. What do you feel are the greatest threats to Los Angeles as we look forward over the next five years?***

   I believe the greatest threats of terrorist attack in the Los Angeles area are those that have proven successful elsewhere in the world. The Los Angeles International Airport, the Ports of Los Angeles and Long Beach and the transit system in Los Angeles County are all vulnerable. The history of Al Qaida aggression is that of returning to finish previously unsuccessful target assaults. The attacks of 9/11 were preceded by an attack in 1993 of which its mastermind, Ramzi Yousef, considered a failure due only to a lack of money and explosives. Similarly, the Bojinka plot of the early 90's was revisited in London only a few months ago with the plan to bomb ten U.S. airliners while in flight. With this in mind, we must assume that prior targeting of the Los Angeles International Airport is still a viable threat. An attack on LAX achieves the goals of economic disruption, destruction of a symbolic site and the potential for mass casualties. Additionally, transit sites have been very attractive to terrorists who have achieved successes in London and Madrid.

   The Ports of Los Angeles and Long Beach are similarly attractive to our enemies. A tremendous economic impact would occur should these hubs of commerce be rendered uninhabitable. During the Longshoreman's Union action of a few years ago, it was estimated that nearly a billion dollars per day was lost to the cessation of port operations. A successful attack on either port would have huge economic repercussions that would be felt worldwide. Other potential attacks against Los Angeles are only limited by one's imagination. Los Angeles is home to hundreds of international companies as well as being the hub of western entertainment companies that export their products worldwide.

3. ***I want to focus on two successes in particular that you have shared with the Committee. In your testimony, you mentioned 2 programs already implemented in LA County. One is the Terrorism Early Warning System that is already operating in 25 different locations in LA County. The other is the Joint Regional Intelligence Center which has brought Federal law enforcement officials together with all Southern California police agencies to share intelligence information.***

What are your recommendations on how the Federal government can help these systems become models for other law enforcement agencies around the country?

These two model programs (Terrorism Early Warning Group and Joint Regional Intelligence Center) are complementary efforts. The JRIC is where local, state and federal agencies come together for intelligence related analysis and sharing, while the TEW provides the organizational structure, system for processing information, and multi-disciplinary component which joins experts from law enforcement, fire, public health and emergency medical services. The JRIC is the first and (currently) only "fusion center" operation to officially have an assigned DHS analyst, along with the FBI and other federal, state and local agency representatives. It incorporates the 18 recommended Global Justice Guidelines and expands that capacity through the attributes of the TEW model.

The mechanism to replicate this successful endeavor is already in place at the National TEW Resource Center located at the JRIC facility. This effort is currently funded by the DHS Office of Grants and Training (G&T), but is not being utilized to its full potential. This center has the capability to be a primary coordinator for enhancing connectivity among all existing information sharing initiatives. Through their efforts, there are currently 26 fusion centers across the nation that have adopted the TEW concept. This established system should be the foundation upon which fusion centers across the country should continue to build.

As I recommended in my original written testimony, it is critical to the formation of a common nationwide information sharing network that this center maintains its existence and increases its funding. These will enable the Center to provide information and technical assistance to all regions that either have, or desire to establish, local, regional or state fusion center operations. It can also serve as a clearinghouse to provide information on all similar initiatives across the country to better incorporate best practices and lessons learned, thus enhancing existing efforts for a seamless exchange of information among all partners in the Global War on Terrorism.

4. ***With regards to intelligence information sharing, some experts believe that the number of appropriate security clearances being issued to local law enforcement officials in order to share and receive vital intelligence from the federal government is far too low. This inability to have access to threat information could lead to local law enforcement officials not being able to receive information on potential terrorist activity which would be critical in helping them to do their jobs and protect local communities. Do you share this view?***

I do not believe it is the number of clearances that is the issue, but rather the timeliness in receiving appropriate clearances. Delays in granting national security clearances may keep important information from reaching the appropriate recipients in a time of impending catastrophe. The need to have access to vital threat related information at the local law enforcement level is essential. While there is no shortage of open source information on the current threat picture, it is crucial for local law enforcement practitioners to be able to compare that information against classified intelligence to get the most accurate situational awareness picture. The local police officer, sheriff's deputy, firefighter or public health nurse will be the first to prevent, disrupt or mitigate a terrorism event. Without the ability to direct their efforts based on current threat information, they will remain behind the curve, playing catch-up.

For the members of my department, the process to obtain a Top Secret security clearance from the FBI takes between twelve and sixteen months. This protracted background investigation not only limits my access to up-to-date threat related information, it also impacts my ability to adequately assign personnel to the Joint Terrorism Task Force operating in Los Angeles. I believe the length of time necessary to evaluate personnel for a security clearance must be cut dramatically and that all local law enforcement executives have appropriate access clearance to vital information.

5. ***In any discussion of homeland security concerns, we are always concerned about the Federal government's communication with state and local officials who will more than likely be the first on the scene in the event of a terrorist attack. The Federal government has spent millions of dollars and countless hours developing complicated networks to disseminate information. However, a June report from the DHS inspector general found that only 2% of the 9,500 registered users of the Homeland Security Information Network actually logged on to the system each day.***

   What has been your experience in sharing information with Federal officials? Can you explain why so few state officials accessed the information that has been made available?

   Our experience in sharing information with federal officials has changed significantly over the past few years. In the local law enforcement networks, information is shared easily between agencies as our missions are similar and our task force operations are common. Prior to the tragic events of 9/11, the sharing of information between local law enforcement and federal agencies was poor. These agencies were viewed as "black holes," wherein information would be submitted, but nothing returned to

the submitting agency. There was also the perception among local practitioners of an interest by federal agencies in over-classifying information that required formal approval to disseminate. Since 9/11, federal agencies have made great strides in overcoming their bureaucratic hurdles and share threat information with local agencies on a more consistent basis.

The Joint Terrorism Task Force structure has been instrumental in overcoming many of these obstacles. Utilizing a system of local law enforcement officers, working side by side with FBI Special Agents, has encouraged the breakdown of barriers that existed in the past. Additionally, the FBI in particular has made efforts to keep local law enforcement executives more informed. Each month, the local Field Office briefs its most important cases to an audience of police executives from throughout Los Angeles County. We are continuing to build the relationships through enhanced participation on the JTTF, monthly briefings and collaborative efforts such as the Joint Regional Intelligence Center.

The lack of interest in the Homeland Security Information Network (HSIN) can be traced to a few issues. Comments from the JRIC about this network include "unwieldy", "quantity over quality", "not police friendly", "another form-over-content trick", and "contains meaningless information." Most intelligence analysts assigned to the JRIC have many sources of information cultivated over years of experience. They utilize "Blogs" (Web journals, "E-zines" (electronic magazines), intelligence reports, Internet sites, periodicals, and human sources that have proven accurate over time. It is difficult to insert a new, unproven source of information into an intelligence analyst's workday. Many projects similar to HSIN have been launched and have failed, due mostly to a "publish or perish" mentality. Also, the audience must be defined.

Is the HSIN looking to better inform police executives or does the HSIN have a desire to be a clearinghouse for Homeland Security information? The intent is not clear among the analysts. Simply to post intelligence reports from other fusion centers or from other federal agencies can be viewed as suspect. Analysts are always interested in acquiring new portals to quality information, but they must be worthwhile for continued usage. To their credit, HSIN project personnel are attempting to rectify their situation through contacts with local law enforcement intelligence analysts. If HSIN project personnel are willing to listen closely to real practitioners, they may well gain the audience attention that was anticipated at the project's inception.

6. ***Explain how the Muslim American Homeland Security Congress (MAHSC) can work with others to achieve the goal of educating communities about extremism?***

The Muslim American Homeland Security Congress is a vital component in securing our nation against terrorism, especially with the rise in the threat of "homegrown" Islamic extremists. Communication and education are essential in this area to strive for prevention while protecting civil liberties and impacting hate crimes. We can only accomplish these goals through a partnership with the Muslim American Community.

The MAHSC was established in Los Angeles to provide awareness and education to both the Muslim and general communities to advance relationships and foster cooperation to impact terrorism in America. It affords open lines of communication among its member organizations and the community. It also serves as a forum where Muslim-Americans can clearly articulate their intolerance for terrorism while educating the public on moderate Muslim values. It is our intention to create chapters in other major regions across the nation. The first such chapter will be in Detroit, which has the largest Muslim population in the United States.

As each new chapter is established, the goals of education and communication will be achieved in the local area and across the country, as this becomes a national organization.

Post-Hearing Questions for the Record
Submitted to Dr. Richard A. Falkenrath
From Senator Susan M. Collins

"Homeland Security: The Next Five Years"
September 12, 2006

1. You have described in detail policies and procedures that have worked well in New York. It goes without saying that there are a number of characteristics of both cities that are unique or at least limited to similar, major metropolitan areas.

Of the observations and suggestions that you have made in your testimony today, what lessons have you learned that you believe can be applied to law enforcement departments in other metropolitan areas and even smaller communities across the Nation?

Counterterrorism is a manpower-intensive operation. The heart of the NYPD counterterrorism program is a vigilant, tightly managed police force. Given staffing and fiscal constraints, it is impossible to protect all potential targets around the clock all the time, although there are certain facilities that warrant this. These limitations have led NYPD to engage in rotating, seemingly random personnel deployments. Our deployments are based on threat information and intelligence, but we work hard to avoid patterns. The sudden appearance of a heavily armed Hercules team can disrupt terrorist surveillance and pre-operational planning. Although the scale will be different, this is a key aspect of our program that can be applied anywhere.

Another crucial aspect of counterterrorism is intelligence. Threat information passed from the federal government is important, but so is local intelligence. There is no substitute for the information that can be obtained through local intelligence operations.

Realistic assessment of likely targets and their vulnerabilities is another key aspect of our operation that can be applied elsewhere. This is, once again, driven by the finite nature of our resources. Although there are many possible targets in New York City, NYPD Threat Reduction / Infrastructure Protection teams focus on reducing vulnerabilities at those facilities that are both most critical and most likely to be targeted. This process can lead to some difficult, unpopular decisions, but there really is no other way.

The aforementioned programs are aimed at detection and deterrence. All law enforcement agencies should be prepared to respond should an attack occur. The basis of this preparedness is training. Not all agencies will be able to develop an in-house training capability as NYPD has done. But they can take advantage of training offered by the federal government, private vendors, and larger agencies such as NYPD. The regional counterterrorism training center established by NYPD in 2002 provides training to members of the Department, personnel from neighboring law enforcement agencies and

private sector security personnel. This training model is valuable because it not only delivers necessary training, but also forges contacts and relationships that become very important when agencies must respond cooperatively to large-scale incidents.

2. What in your mind, are the greatest threats facing America over the next five years?

Al-Qaeda and affiliate terrorist organizations remain the primary threat to the U.S. for the foreseeable future. These are the groups with a proven ability to carry out attacks capable of inflicting great harm against the nation. Their desire to do so has not diminished, although some of their capabilities have been degraded due to U.S. and allied efforts around the world. Despite this degradation, these established Islamic terrorist organizations pose the greatest threat. At the same time, however, we must be aware of the potential "homegrown" threat. Islamic radicals exist in the U.S. and radicalizing influences abound. The potential for a group of like-minded individuals to coalesce into a cell capable of perpetrating an attack is real. Such a cell could obtain bomb-making instructions from the Internet or a book and could legally purchase bomb-making materials such as ammonium nitrate. With some skill, this cell could pull off a devastating attack, such as occurred in Oklahoma City in 1995.

3. You have talked about the great progress your respective entities have made in the area of homeland security. There are still, of course, a number of areas where your city could be targeted. What do you feel are the greatest threats to New York City as we look forward over the next five years?

My personal opinion is that the most likely form of terrorist attack against New York City is the simultaneous detonation of multiple man-portable improvised explosive devices in the mass transit system. This attack method has been used successfully in Madrid and London, it is highly effective in sowing terror and providing the visual images terrorists seek for exploitation purposes and it is extremely difficult to defend against. The sheer size of the system and the inherent nature of mass transit increase the system's vulnerability. This is an area where the federal government currently provides very little help to New York City.

4. In any discussion of homeland security concerns, we are always concerned about the Federal government's communication with state and local officials who will more than likely be the first on the scene in the event of a terrorist attack. The Federal government has spent millions of dollars and countless hours developing complicated networks to disseminate information. However, a June report from the DHS inspector general found that only 2 percent of the 9,500 registered users of the Homeland Security Information Network actually logged on to the system each day. What has been your experience in sharing information with Federal officials? Can you explain why so few state officials accessed the information that has been made available?

No. From the NYPD's perspective, the utility of the Department of Homeland Security's information-sharing initiatives is severely limited by DHS's apparent inability to treat various state and local agencies differently according to their role, their sophistication, and their potential contribution to the national mission of combating terrorism. Consequently, NYPD's collaboration with other members of the national intelligence community and with foreign law enforcement and intelligence agencies is substantially more valuable than our collaboration with DHS. The most useful information NYPD receives from the federal government comes to us through our participation in the NY Joint Terrorism Task Force. This is generally case-specific classified information which fills a specific need, but is not sufficient.

5. In your written statement you said, "since September 11, 2001, most terrorist plots and attacks perpetrated worldwide have been conceived, planned, and executed by individuals who are part of the local populace and who have only limited, if any, transnational linkages to terrorist organizations abroad." How can we confront the challenge of home-grown terrorism? How can we work with the American Muslim Community to prevent radicalization of our citizens?

To confront a terrorism threat that is increasingly "homegrown"– that is to say, comprised mostly of self-radicalizing individuals with limited links to the larger international jihadist movement – the U.S. should institute a two-prong strategy. First, we need an effective *domestic* counter terrorism and intelligence program. The U.S. expends much more to combat transnational terrorism abroad than on domestic investigations and operations.

In addition to the federal government, local law enforcement must play a role in combating the homegrown threat. In most cases, a threat that is truly homegrown is more likely to be detected by an investigator with intimate knowledge of his local community, rather than an agent physically removed from the area. I noted in my written testimony that a reformed FBI and a "genuinely *joint* Joint Terrorism Task Force" are vital to the effort, but not sufficient to counter the threat. As a result, other domestic law enforcement entities should follow New York's example and work to expand existing intelligence and counterterrorism apparatuses.

Second, government agencies and non-governmental organizations should work with local Muslim-American communities to address the grievances, alienation, and other issues that may lead to radicalization and extremism. Many counterterrorism experts see a direct correlation between feelings of alienation among Muslim populations and susceptibility to the message of radical Islam.

6. In your written testimony you note that "there is no area of the Department's work that disappoints [you] more than critical infrastructure protection." You go on to discuss in your testimony what the NYPD is doing at the local level to enhance the security of New York's critical infrastructure. For the moment, I am interested in what DHS should be doing in order to successfully implement its critical

infrastructure mission. Can you provide your assessment to the Committee as to what the Department needs to do to improve its efforts for its critical infrastructure mission?

There are many different ways in which DHS can improve its critical infrastructure efforts but the following four are worth mentioning. First, the Department should deal directly with the agencies most knowledgeable of, and most involved in, the protection of critical infrastructure, rather than working through ill-informed intermediaries. Second, the Department should focus its critical infrastructure protection resources on a limited number of high priority, high density target areas, other than spread them thinly across the country to avoid political criticism. Third, the Department should recommend a design basis threat and blast performance standard for all major new buildings for inclusion in local building codes. Finally, the federal government should intervene in the insurance market to promote private-sector terrorism insurance. Buildings meeting certain standards would qualify for lower insurance rates. This would drive property owners to increase their investment in security.

Post-Hearing Questions for the Record

Submitted to Steven N. Simon

From Senator Susan M. Collins

"Homeland Security: The Next Five Years"

September 12, 2006

1. In keeping with the theme of the hearing, "Homeland Security: The Next Five Years," what are the greatest threats facing our country in the next five years?

Answer:

My view on this question is rather narrow, but having said this, my biggest concern would be a terrorist attack that led to further erosion of civil liberties and to tensions between Muslim and non-Muslim Americans.

What policies should we, as a nation, be implementing to combat these threats and mitigate the consequences?

Answer:

Withdraw from Iraq; restore Alliance relations; act generously but in a way consistent with our other strategic commitments to remedy Muslim grievances, in particular by seeking a resolution of the Palestinian crisis; restore a balance between our emphasis on military counter-terrorism and the use of law enforcement, intelligence, diplomacy, economic assistance, trade, etc.; consistent with our values, do what is necessary to sustain the cooperation of friendly, but authoritarian governments; urge Musharraf to broaden his political base, such that his ability to deal with the insurgency in the FATA is sustainable; allocate greater resources to Afghanistan; devote serious attention to proliferation of nuclear and radiological materials, components and subcomponents; deploy a usable special operations capability that can pursue the adversary in hostile environments without the backing of a large and politically untenable expeditionary force; attempt a limited reform of the IC by getting clandestine service officers out of embassies and by restoring a strategic analytical capability to the community; improve communication between the FBI and local law enforcement, while radically upgrading the ability of local law enforcement to learn about and interact with Muslim communities within their jurisdictions.

2. You have previously described what you view as the evolution of the jihad movement into a form of urban warfare. What measures can we take to combat this evolving threat?

Answer:

This will require more cops on the beat, meaning better funded, equipped, and informed police work – assisted as necessary by national level intelligence enforcement. It will also require a vastly more comprehensive camera surveillance network in municipal areas, such as London has implemented. There is currently insufficient funding for this well understood and easily deployable technology. In addition, the public will have to be more vigilant regarding such threats as car and truck bombs and suicide bombers. Increasing awareness without precipitating panic, or, worse, indifference, will be a serious challenge to the country's leadership.

3. We now know that many of the would-be hijackers involved in the London plot were so-called "home-grown" terrorists without clear links to international terrorist organizations. How can we win the hearts and minds of the Muslim community which would help prevent "home-grown" terrorism?

Answer:

The London attackers did have international terrorist connections, but it is both true and disturbing that their radicalization preceded these contacts. The American Muslim community is our most valuable asset in the war against terror. Their patriotism should not be taken for granted. According to 2007 Pew polling, large pluralities or small majorities believe that the war on terror is a war against Islam and that al Qaeda did not destroy the World Trade Center towers. There is also little reason to believe – against this background – that Muslim youths should be any less amenable to web-borne propaganda than their European counterparts, despite the large socio-economic differences between them. The American Muslim community is subject to a greater degree of prejudice as a result of 9/11 and of a strand of resurgent Protestant evangelicalism that emphasizes religious boundaries and delegitimizes competing faiths. Among the things the US can do is avoid indiscriminate responses, such as large scale arrests as occurred after 9/11; avoid scurrilous, overzealous, or incompetent prosecutions that fuel the belief that Muslims are being "set-up." This means making more careful, responsible use of informants. Also important is greater attentiveness to Muslim foreign policy concerns particularly on Iraq and Palestine. This does need not entail wholesale reversals in policy, but rather a consistent demonstration that Muslim concerns are heard and are taken into account.

4. In your latest book, you argue that the integration of the American Muslim Community into the larger fabric of America is fundamental to our continued security. You also point out that the Muslim communities in Europe are largely isolated and alienated from the culture of their host country. You argue that the cultural isolation makes those communities more susceptible to jihadist ideology. Can you explain to us why you believe that to be the case and what we can learn from the European experience?

Answer:

When minority communities perceive themselves to be under threat, they erect boundaries, forming what Israeli scholar Emmanuel Sivan calls "enclave cultures." These communities become preoccupied with boundaries and the need to police them by discouraging defections from the group. These defensive arrangements, in turn, feed perceptions of the majority in the society that there is something wrong with the minority population; that the minority group wishes to be different and disdains majority values. A dangerous feedback loop is created which intensifies social divisions. As this process unfolds, moderates leaders in the minority group are increasingly unable to "deliver the goods" in the form of greater social tolerance, opportunity, and political influence for their constituents. This opens the door to a more militant figures, who can compete, often successfully, for leadership of all or key segments of the minority population. Intercommunal tensions—and the potential for violence – grow as a result. Europe is nearing a tipping point in this regard.

This is why it is imperative that lines of communication with Muslim communities in the US be kept wide open and Muslims are made to feel as though their views count and their voices are heard.

5. You have predicted that the terrorists are committed to attacking the homeland with a Chemical, Biological, Radiological, or Nuclear device. Such an attack would have a devastating psychological impact as in addition to the destruction directly caused by such an attack. What we should be doing right now to prevent such an attack or at least mitigate its effects?

Answer:

Prevention is all in the realm of effective intelligence work, good liaison ties with foreign services, and effective border controls. All these areas in need of improvement.

It is essential that if an attack does occur, that both the American people and our adversary see the US government respond swiftly, effectively and compassionately to contain the damage, restore services, treat the injured, and maintain order. As the response to Hurricane Katrina demonstrated, federal authorities, as currently constituted and equipped, would be unable to respond in a way that secured the confidence of an anxiety stricken citizenry and the respect of our adversary. As the well known homeland security "Report Card" made clear, in the 11 of 13 categories of consequence management capability, the current administration warrants grades C through F. When this report is set against the backdrop of our failing health care delivery system, which is rapidly losing the excess capacity that would be desperately needed in the event of a mass casualty attack we are in a very precarious position.

As a first step, Washington needs a strategy that reflects the concerns and limits of jurisdiction outside of Washington. Such a homeland security strategy has yet to be

produced; all we have is a "gameplan," which has been disavowed by the local authorities who would have to implement it.

Second, the USG should establish standards for state and local response capabilities, inventory the existing capacities of likely target cities, and then proceed immediately to remedy shortfalls. These localities will have to deal with a desperate situation alone until federal capabilities can be brought to bear – as 9/11 demonstrated in New York City. They are the first line of defense.

Third, local police capabilities as well as intelligence access must be upgraded, and surveillance systems deployed.

Fourth, Washington must take a strategic view of our health care system and maintain excess capacity in which the market is uninterested.

Fifth, dangerous installations that are co-located with cities must be rendered safe through implementation of alternative production techniques. Chlorine plants are a prime example.

Post-Hearing Questions for the Record
Submitted to Daniel B. Prieto
From Senator Susan M. Collins

"Homeland Security: The Next Five Years"
September 12, 2006

1. In keeping with the theme of the hearing, "Homeland Security: The Next Five Years," what are the greatest threats facing our country in the next five years?

Three major factors will pose significant challenges in the coming years.

First, the threat of weapons of mass destruction (WMD) proliferation will increase. The growing challenge comes from North Korea's pursuit of nuclear weapons and the push by Iran to acquire nuclear weapons capability. The involvement by non-state actors, like the A.Q. Khan supply network, in the proliferation of WMD-related technologies, weapons design, and equipment will continue to grow in seriousness. We will also be challenged by terrorists' efforts to acquire and use weapons of mass destruction, a situation made more dangerous by potential cooperation between terrorists and rogue or weak states possessing WMD and related technologies.

Second, the terrorist threat continues to evolve. Al Qaeda suffered significant blows to its central leadership and organization after 9/11, leading intelligence officials to suggest that much of Al Qaeda's central leadership had been neutralized and that the primary national security threat came from splinter groups that were inspired, but not commanded by Al Qaeda. In July 2007 the Office of the Director of National Intelligence released a National Intelligence Estimate (NIE) that concludes that Al Qaeda "has protected or regenerated key elements of its Homeland attack capability" by recovering from the loss of Afghanistan as a safehaven, reestablishing a haven in Pakistan's Federally Administered Tribal Areas (FATA), and reconstituting its leadership with a new cadre of operational lieutenants and senior leadership to replace the founding leadership generation.[1] The report also notes that Al Qaeda has been able "to recruit and indoctrinate operatives, including for Homeland attacks," by associating itself with an Iraqi subsidiary, Al Qaeda in Iraq (AQI).[2]

The NIE characterizes Al Qaeda 2.0 as a new series of decentralized, independent, self-generating and increasingly home-grown cells in Western countries and potentially the United States which are not necessarily operationally linked to Al Qaeda central. This is exemplified by the perpetrators of the London transit bombings in July 2005 and the thwarted London-based plot to target transatlantic flights in August 2006. Such cells present a significant challenge to security forces and will be a significant resource to Al Qaeda central.

Furthermore, the speed of radicalization has accelerated. The war in Iraq has spurred recruitment to radical Islamist groups.[3] The rapid growth of alternative media outlets and terrorists' use of the internet increase the availability of propaganda and training.

---

[1] Office of the Director of National Intelligence, "National Intelligence Estimate: The Terrorist Threat to the US Homeland," 17 July, 2007, available at: http://www.dni.gov/press_releases/20070717_release.pdf
[2] ibid.
[3] DeYoung, Karen, "Spy Agencies Say Iraq War Hurting U.S. Terror Fight," Washington Post, September 24, 2006, p. A01.

Third, whenever and however the war in Iraq winds down, it poses a significant threat to the United States and its allies. Like Afghanistan was for Bin Laden in the 1980s, Iraq has provided a theater for the next generation of terrorist leaders to make connections, and build rolodexes and reputations. Iraq has provided a training ground for a new generation of terrorists to hone bomb-making techniques, tactics against military personnel, and tactics against critical infrastructure targets. Between May of 2003 and September, 2006 there were over 356 attacks on Iraqi oil and gas pipelines and installations.[4] Dozens of attacks used explosives to target and weaponize chlorine gas in trucks. Numerous additional attacks targeted the electrical grid[5] and water facilities.

As the Iraq war winds down, the situation will be analogous the late 1980's, which saw a Soviet retreat from Afghanistan. Alumni of the jihad against the Soviets brought terrorist tactics back to their home countries and formed the nucleus of what was to become Al Qaeda.

2. What policies should we, as a nation, be implementing to combat these threats and mitigate the consequences?

In order to address the dynamic threat environment, there are five critical areas for improvement in the realm of homeland security. Additional detail on each of these is available in my full written testimony.

1) **Engage Society, Educate the Public and Enlist the Private Sector.** To date, we have not done nearly enough to educate the public or to sufficiently engage the resources and goodwill of the private sector. We must encourage and empower the public on homeland security issues and ensure that the private sector works in much fuller partnership with the government to protect the country.
2) **Move from Tactics to Doctrine.** Numerous homeland security strategy documents since 2001 have provided tactics, methods and processes, but have failed to articulate strategy and doctrine that provide clear guidance for implementation and goals by which we can measure progress. Homeland security strategy must articulate a coherent vision with measurable goals. DHS must establish a clear doctrine of national preparedness that requires us to be ready to address multiple simultaneous high-consequence events. DHS should strive to make critical infrastructure secure through a mix of government incentives, standards and regulations. Diverse investments in security will improve the overall health of American critical infrastructure, providing long-term benefits to our overall economy and society.
3) **Ensure DHS Succeeds**. We can not afford to have a weak DHS that lacks credibility and is challenged to carry out its mandate. One of the major problems DHS has faced is weak management of a complex merger integration process. This needs to change. We should strive to ensure that DHS is a healthier and more respected organization, equal to the task Americans expected of it when it was created. Congress should ensure that DHS management has the right level of expertise, is well resourced, and has clear authorities and goals. Congress should urgently follow the recommendations of the 9/11 Commission to reorganize itself and streamline the number of congressional committees that DHS has to report to.

---

[4] O'Hanlon, Michael, "Iraq Index: Tracking Variables of Reconstruction and Security in Post-Saddam Iraq," October, 2006, available at http://www.brookings.edu/fp/saban/iraq/index.pdf.
[5] http://www.defenselink.mil/news/Sep2004/n09162004_2004091611.html

4) **Get Technology Right.** While the U.S. is the envy of the world when it comes to technology, the federal government struggles to implement important homeland security technology projects and to effectively deploy valuable everyday technologies in the homeland security realm. The government should make sure that it leverages the best of American technology prowess and innovation and partners with top-notch technology executives, professionals and managers to support the effort.

5) **Improve Information Sharing.** Increased information sharing will help prevent terrorist attacks and also aid in responses to domestic disasters as well. We need to make sure that information sharing efforts improve the quality of homeland security decisionmaking and do not simply flood homeland security professionals with more information. When it comes to information sharing, quality is paramount, not quantity. Furthermore, information sharing efforts must proactively address civil liberties concerns.

3. We now know that many of the would-be hijackers involved in the London plot were so-called "home-grown" terrorists without clear links to international terrorist organizations. How can we win the hearts and minds of the Muslim community, which would help prevent "home-grown" terrorism?

The susceptibility of indigenous Muslim communities in Europe to terrorist radicalization is a vexing problem that will last for more than a generation. The United States and its allies must develop effective strategies to address the threat of home-grown extremists originating within immigrant communities and bent on attacking their own countrymen. Successful policies will be less about winning hearts and minds since many members of immigrant Muslim communities are likely to maintain sharp disagreements with U.S. policies in the Muslim and Arab world. What will be more important is to prevent *losing* hearts and minds to a radical Islamist ideology that advocates violence.

While military efforts and aggressive intelligence and police work are the right tools against terrorist operatives, such tactics are insufficient to address terrorism's root causes or to counter terrorism in the earlier stages of recruitment and radicalization. If we are serious about countering terrorism, we must bring every possible tool to bear and exploit the full range of policies and national capabilities. To address home-grown terrorist threats, it is essential to address terrorism in its life cycle at earlier stages and well before terrorist cells start planning and become operational. Policies must include improving education, increasing economic opportunities, improving community outreach and bettering relations with police.

There are four primary stages in the "life cycle" of a terrorist. Each step offers policymakers an opportunity to deter, "turn" or counter potential terrorists.

> **Stage 1: Alienation from broader society.** The terrorists who undertook the July, 2005 bombings in London were relatively mainstream by British standards. They had attended high school or college. They all held jobs. Two were married, with two others living with close relatives. Yet, despite these social ties and seemingly "normal" backgrounds they still became suicide bombers. Indeed, many homegrown terrorists appear to be well integrated into society. Many come from middle class backgrounds. Few are

economically destitute. Many have some form of higher education.[6] For individuals susceptible to radicalization, feelings of alienation are often a function, first of a desire to be part of the western societies in which they live, followed by subsequent feeling of rejection by and rejection of the west. With the London bombers of 2005 and again with the 2006 plotters, either overt experiences of discrimination or generalized feelings of lack of belonging led to feelings of alienation that prevented the bombers from forging a durable British identity.

Stage 2: Search for identity/Transnational identity. In response to their sense of alienation, subjects search for a sense of meaning and belonging. To do this, they conduct research and seek out sources of information and education. Subjects often turn to the internet and encounter radical Islamist websites, propaganda videos and other materials.[7] Online materials combine with existing feelings of alienation to fuel a sense of anger, humiliation, and a sense of powerlessness. After encountering these materials and exhibiting an interest in them, disaffected individuals will seek new social relationships. Individuals start to fall into radical social networks as they seek affirmation and to forge a sense of community belonging. The venues for making these connections can be either virtual (e.g. online chat rooms) or physical (e.g. discussion groups at the local mosque). Growing social affiliations result in a gradual intensification of religious beliefs. In this stage of the process, individuals increasingly become de-nationalized and increasingly identify themselves as part of a global community and global movement.

Stage 3: Group cohesion. As they become increasingly radicalized, individuals will retreat into small groups of like-minded individuals. Individuals within these groups quickly form a shared group identity based on close bonds of friendship, a shared sense of alienation and isolation from the community and society around them, and a shared resentment at Western domination and Muslim victimhood. Bonds deepen to reinforce the individual's relationship with the group and with a transnational Islamic identity. The strong sense of group solidarity and a new sense of transnational identity dilute outside relationships which might otherwise act as a moderating force. Once formed, these groups form the basis of what could become a terrorist cell. The London bombers, the Montreal cell which attempted to carry out a bombing of the Los Angeles airport, and the Hamburg cell which carried out the 9/11 attacks initially formed as groups of friends and drifted into terrorism. In the case of the Hamburg cell, it was identified by senior Al Qaeda leadership as having the human capital and capabilities necessary to carry out the planed attack. It is important to note that while the Montreal and Hamburg cells had received military training, the 2005 London bombers had not, as training opportunities had been disrupted by the American intervention in Afghanistan.

Stage 4: Mobilization. Once small self-starting groups have formed, one of three things can happen: the group disbands on its own; top-down recruitment takes place (e.g. the 9/11 Hamburg cell); or the group self-mobilizes, and carries out an attack on its own (e.g. the 2005 London bombers). In the recruitment cases, it is critical to note that physical meetings with recruiters need never take place and that internet recruitment is becoming

---

[6] Silber, Mitchell and Arvin Bhatt, "Radicalization in the West: The Homegrown Threat," New York Police Department, July 2007, available at http://www.nyc.gov/html/nypd/pdf/dcpi/NYPD_Report-Radicalization_in_the_West.pdf

[7] Henry, Terrence, "Get Out of Jihad Free," *The Atlantic Monthly*, June 2007. http://www.theatlantic.com/doc/200706/saudi-jihad

> prevalent. Saudi officials estimate that 80% of terrorist recruitment takes place on the internet.[8] According to senior Egyptian counterterrorism officials, nearly all of the individuals involved in the nine significant terrorist conspiracies in the last two years were recruited and trained over the internet.[9] In the "self-mobilizing" cases, it is important to note the lack of recruitment by an outside group and the lack of training or command and control from some outside organization. In the "self-mobilizing" cases, the catalyst for the shift from simple disaffection to the actual plotting of an attack is self-generated. The members in the group feed off each other, become increasingly radicalized, and independently develop their own plan for an attack. One member alone can often instigate preparations for an attack. Other members of the group are, in effect, hostage to the most radical group member. The strong bonds of group solidarity prevent single individuals from backing out and letting down the other members of the group.

The distinct stages of terrorist radicalization and recruitment present multiple opportunities for policy solutions.

To address the early stages of disaffection, governments need to undertake measures to improve the cultural and economic assimilation of new and second- or later-generation immigrants. Job training programs, education assistance and public awareness campaigns should be undertaken to support better integration of immigrants into societies and to improve relationships between immigrant communities and host countries.

In the second stage, Al Qaeda and radical Islamist propaganda and materials are available in open-source venues. Governments should be able to disrupt websites to make it more difficult to obtain propaganda, training and other source material. Governments should also work closely with moderate Muslim groups to develop content and participate in online venues and at mosques to counter and provide alternatives to radical messages. Governments should also work closely with moderate Muslim groups to sideline radicals and seek to deport radical Imams if necessary. However, it is important for government officials to tolerate and allow for significant disagreement with moderates, so as not to undermine the legitimacy of moderate groups within immigrant communities. Advocacy of violent activity, not policy disagreements, should be the measure by which governments measure websites, publications, and community activists. Members of Muslim communities must themselves do more to turn their own against extremism. This is harder said than done, though: European Muslims who have been seen to be cooperating with government authorities have often lost credibility in their communities.

As groups become more radicalized in the third stage, increased monitoring by intelligence and law enforcement agencies is essential. While many groups are sympathetic to terrorism, most will not make the jump towards violence or active measures to support terrorism. Security services need to keep close watch on local networks in order to detect preparations or moves in the direction of violence. Government authorities will also need to pursue active measures to disrupt groups and discredit members. It is important that these efforts be subtle so as not to alienate the broader Muslim community. To the maximum extent possible, efforts should be sure to respect immigrant cultures and rights and be pursued in a way that they are not viewed as based on racial bias. This can be best ensured where government and law enforcement authorities have longstanding relationships with members of the community. Community relationships will

---

[8] al Saleh, Huda "Saudi Arabia: Internet Most Popular Terrorist Recruitment Method," *Asharq Al-Awsat*, 2 May, 2007. Available at http://www.asharqalawsat.com/english/news.asp?section=1&id=8837

[9] Prieto, Daniel B., not-for-attribution conversation with senior Egyptian counterterrorism official, June 2007.

also be essential if there is to be any chance to pursue last-ditch opportunities to appeal to radicalized individuals through family members or other members of the community. As well, it will be very important for government authorities to work with moderate groups to counter radical beliefs with alternative interpretations of Islam and with productive opportunities and activities that might provide an alternative to radicalization.

In the fourth stage, traditional intelligence and law enforcement techniques are essential to counter terrorist groups once they have decided to mobilize and have entered planning stages towards operations. This will be most effective when government authorities have invested in building relationships with immigrant communities so that members of the community will be more likely to alert authorities to potential threats. Governments should seek to build these relationships by building an honest, open, dialogue with their Muslim communities.

Solutions will require patience and perseverance from societies that want security now. They will also require greater engagement by European societies of immigrant communities that they have traditionally tolerated but which they have not effectively integrated.

4. Several witnesses emphasized the need to focus more on securing our critical infrastructure and planning for how to restore that infrastructure in the event that it is attacked. What advice would you give DHS in formulating plans for critical infrastructure sectors?

The Homeland Security Act of 2002 defines critical infrastructure "as systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." The Homeland Security Act not only defines what critical infrastructure is, but also requires DHS to identify priorities for critical infrastructure, develop a comprehensive national plan, and recommend protective measures.

The latest version of the National Infrastructure Protection Plan (NIPP) fails to meet these requirements. The NIPP identifies obvious, if important tactics – public-private partnership, information sharing, and risk management – but does not provide the kind of sufficient strategic guidance that can coherently guide resource allocation and programmatic activities. We continue to lack a comprehensive strategy for critical infrastructure that meets the requirements of the Homeland Security Act. Additionally our critical infrastructure efforts suffer from a number of other shortcomings.

First, DHS has generally assumed that the market would provide sufficient incentive for companies to adequately protect critical infrastructure. That has not happened. Washington needs to step up to make sure that we protect critical infrastructure better.

Second, DHS was not granted new authorities, other than what it inherited from legacy offices, for security over vital critical infrastructure sectors. Recent legislation to grant DHS interim regulatory authority over the security of some segments of the chemical industry is a step in the right direction, but more needs to be done. DHS needs to be given authority over security activities at any infrastructure sites that threaten large-scale casualties or are critical to the functioning of the U.S. economy, regardless of sector. So, for example, DHS should have the authority to regulate critical energy infrastructure sites in order to mitigate known vulnerabilities in the electric grid.

Third, Washington has fallen into a kind of "political correctness" over critical infrastructure, as if all sectors pose equal risks. They do not. We must come to consensus on which sectors are more important than others. HSPD-7 started in this direction when it recommended prioritizing critical infrastructure that would have WMD-like effects if attacked. Secretary Chertoff also moved in the right direction when he talked about the importance of risk-based allocations for grant funding. But the failure to definitively establish and articulate clear priorities has been evident in DHS' miscues over the national critical infrastructure database and reductions of grant funding to Washington, DC and New York.

Prioritization of CI sectors should be based on:

> **Vulnerability and Consequence.** What industries best provide the top three terrorist goals: casualties, symbolism/theater, and economic impact?
>
> **Companies' Ability to Address Vulnerability.** Some industries are more capable than others of implementing significant security enhancements on their own and in the near term. The industries least able to protect themselves are those: 1) that exhibit low growth, low profit margins and tight cashflow, all of which limit capital available for investments; 2) whose businesses rely on long-lived capital assets, which are difficult to retrofit or replace easily; and 3) that are not tightly regulated and, therefore, lack a quick mechanism by which the government can simply mandate greater security.
>
> **Geography.** Further critical infrastructure prioritization should also give significant consideration to the geographic location, concentration, and interconnectedness of critical infrastructure.[10]

These criteria indicate that the top priorities for critical infrastructure protection are chemical facilities; transportation, including airlines, ports, mass transit, and hazmat transport; and energy, including oil, gas, and the electric grid. It also indicates that the greatest focus should be paid to such facilities in close proximity to major metropolitan areas with a combination of high population density and high symbolic value.

Fourth, DHS should work with Congress to increase monies dedicated toward protection. DHS has sharply curtailed its critical infrastructure efforts so that it is now acting largely as a coordinator for the efforts of other agencies. This is a mistake, and falls short of the mission Congress and the public expected. In 2004, DHS directed $300 million to critical infrastructure protective actions, including pilot programs, technology applications, bombing prevention, security training and community security planning. In FY07, only $30 million was requested for protective actions, a reduction of 90 percent in three years.

Fifth, DHS should work with Congress to provide tax incentives to boost companies' investment to protect critical infrastructure. Washington needs to better use all of the policy tools at its disposal to enhance the security of critical infrastructure. The government should creatively use tax policy to promote additional security investments to the extent that it believes that industry, on its own, is not investing enough. For example, the chemical industry is often criticized for not

[10] Parfomak, Paul W., "Vulnerability of Concentrated Critical Infrastructure: Background and Policy Options," Congressional Research Service, December 2005. For an excellent discussion of risk analysis as well as a ranking of the terrorism risks faced by individual U.S. cities see Willis, Henry, A. Morral, T. Kelly, and J. Medby, *Estimating Terrorism Risk*, RAND Corporation, 2005.

taking enough action to improve security after 9/11. Such a critique fails to give industry credit for the $3 billion that major chemical manufacturers have spent since 9/11 to enhance security. The private sector takes security seriously and has made significant investments. If society believes that more security is warranted -- over and above good-faith efforts already being pursued by the private sector -- the government should help catalyze greater investment by providing tax incentives.

Improving the security of critical infrastructure is essential to homeland security. Moreover, security investments in infrastructure can benefit the U.S. economy and society over the long term. Such "positive externalities" should not be overlooked as the government considers policies to catalyze greater levels of investment in infrastructure security. It is important to remember that the U.S. interstate highway system was built for security reasons and that the Defense Department was responsible for building the networks and technologies that eventually became the Internet. Security considerations have always played a significant role in national investments in infrastructure. There is no reason that the same should not be true today.

America's global economic rivals China and India are investing scores of billions of dollars into the transportation, energy, and communications infrastructures that will power their economies for a generation. America's infrastructure would benefit from comparable levels of investment. The American Society of Civil Engineers in 2005 provided a national report card on the health of U.S. infrastructure.[11] With an average grade of "D" for aviation, bridges, dams, energy, rail and transit, among others, U.S. infrastructures are more vulnerable to terrorist attack or natural disasters than then they should be, and they will have a harder time recovering after an event. The United States can not and should not make due with decades old infrastructure that is brittle and in poor health.

[11] American Society of Civil Engineers, *Report Card for America's Infrastructure*, 2005, available at http://www.asce.org/reportcard/2005/index.cfm.